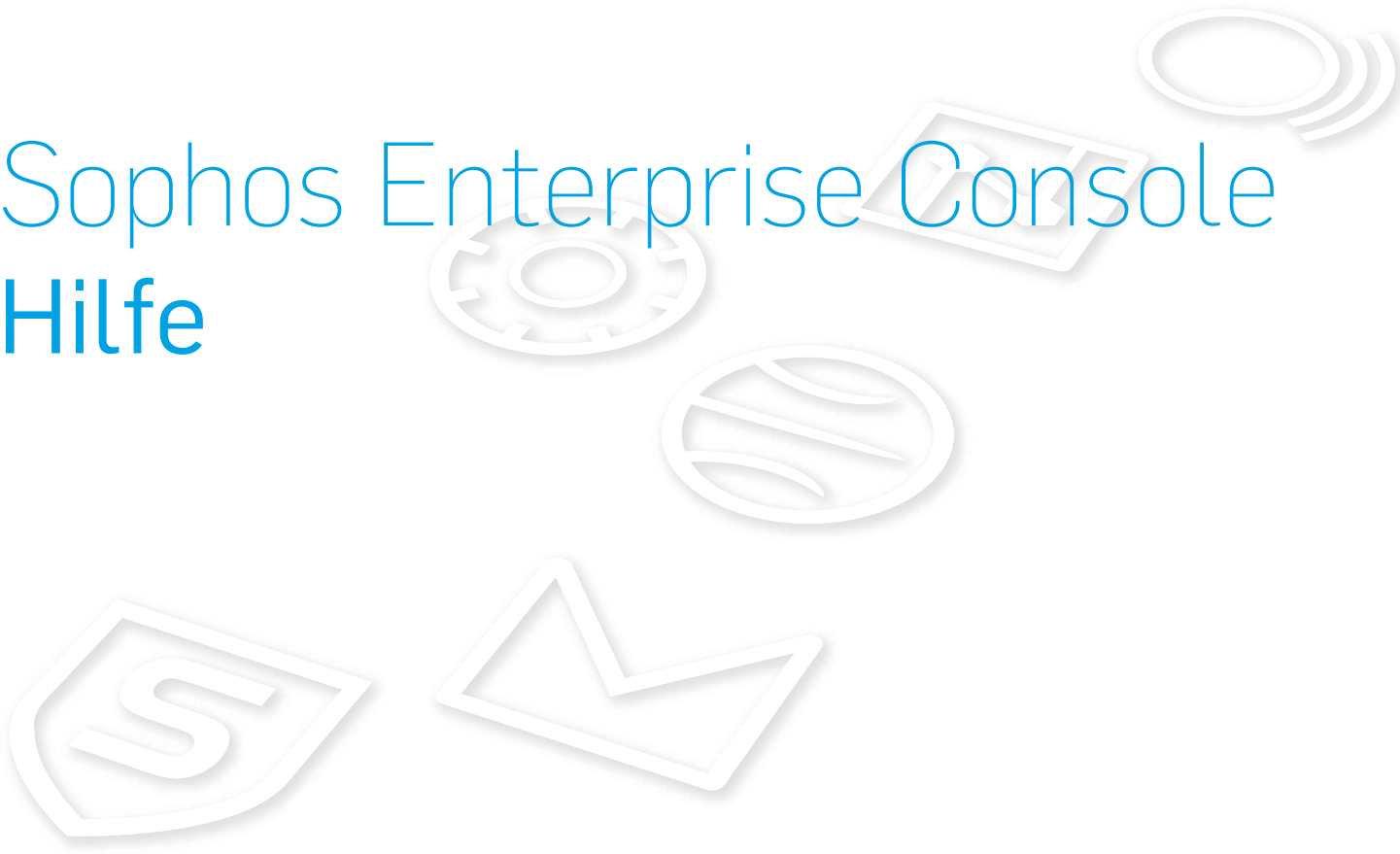
SOPHOS

simple + secure

Sophos Enterprise Console
Hilfe



Produktversion: 5.1
Stand: Juni 2012

Inhalt

1 Über Enterprise Console 3
2 Übersicht über die Oberfläche von Enterprise Console....4
3 Erste Schritte mit Sophos Enterprise Console....14
4 Einrichtung von Enterprise Console....17
5 Schützen von Computern....49
6 Updates....69
7 Konfigurieren von Richtlinien....94
8 Einrichten von Alerts und Benachrichtigungen....201
9 Ereignisanzeige....212
10 Erstellen von Reports....223
11 Wiederherstellen des Zugangs zu verschlüsselten Computern....235
12 Kopieren und Drucken von Daten mit Enterprise Console....238
13 Fehlersuche....240
14 Glossar....248
15 Technischer Support....256
16 Rechtlicher Hinweis....257

1 Über Enterprise Console

Bei Sophos Enterprise Console, Version 5.1, handelt es sich um eine eigenständige, automatisierte Konsole, mit der Sophos Sicherheitssoftware unter Windows, Mac OS X, Linux und UNIX verwaltet und upgedatet wird. Enterprise Console umfasst die folgenden Funktionen:

- Schutz des Netzwerks vor Viren, Trojanern, Würmern, Spyware, schädlichen Websites, unbekannten Threats, Adware und sonstigen potenziell unerwünschten Anwendungen.
- Kontrolle der aufgerufenen Websites, weiterer Schutz des Netzwerks vor Malware und Verhindern, dass Benutzer unangebrachte Websites aufrufen.
- Kontrolle der Anwendungen, die im Netzwerk ausgeführt werden dürfen.
- Verwalten des Client Firewall-Schutzes auf Endpoints.
- Bewerten der Konformität von Computern mit den festgelegten Bedingungen vor der Anmeldung im Netzwerk und Richtliniendurchsetzung.
- Überprüfen von Computern auf fehlende Patches.
- Verhindern unerwünschter Datenverluste von Endpoints (z.B. versehentliche Übertragung sensibler Daten).
- Verhindern, dass Benutzer nicht zugelassene externe Speichermedien und Wireless-Geräte auf Endpoints einsetzen.
- Verhindern, dass Benutzer Sophos Sicherheitssoftware umkonfigurieren, deaktivieren oder deinstallieren.
- Schützen von Daten auf Endpoints vor unbefugten Zugriffen dank Festplattenverschlüsselung.

  Hinweis: Diverse Funktionen sind nicht in allen Lizenzen enthalten. Wenn Sie sie nutzen möchten, müssen Sie eine entsprechende Lizenz erwerben. Nähere Informationen finden Sie unter *http://www.sophos.com/de-de/products/complete/comparison.aspx*.

2 Übersicht über die Oberfläche von Enterprise Console

2.1 Komponenten der Benutzeroberfläche

Die Benutzeroberfläche von Enterprise Console setzt sich aus folgenden Bereichen zusammen:

Symbolleiste

Die Symbolleiste umfasst Verknüpfungen zu den häufigsten Befehlen zur Verwendung und Konfiguration von Sophos Sicherheitssoftware.

Weitere Informationen finden Sie unter *Schaltflächen der Symbolleiste* (Seite 5).

Dashboard

Das **Dashboard** zeigt den Sicherheitsstatus des Netzwerks auf einen Blick an.

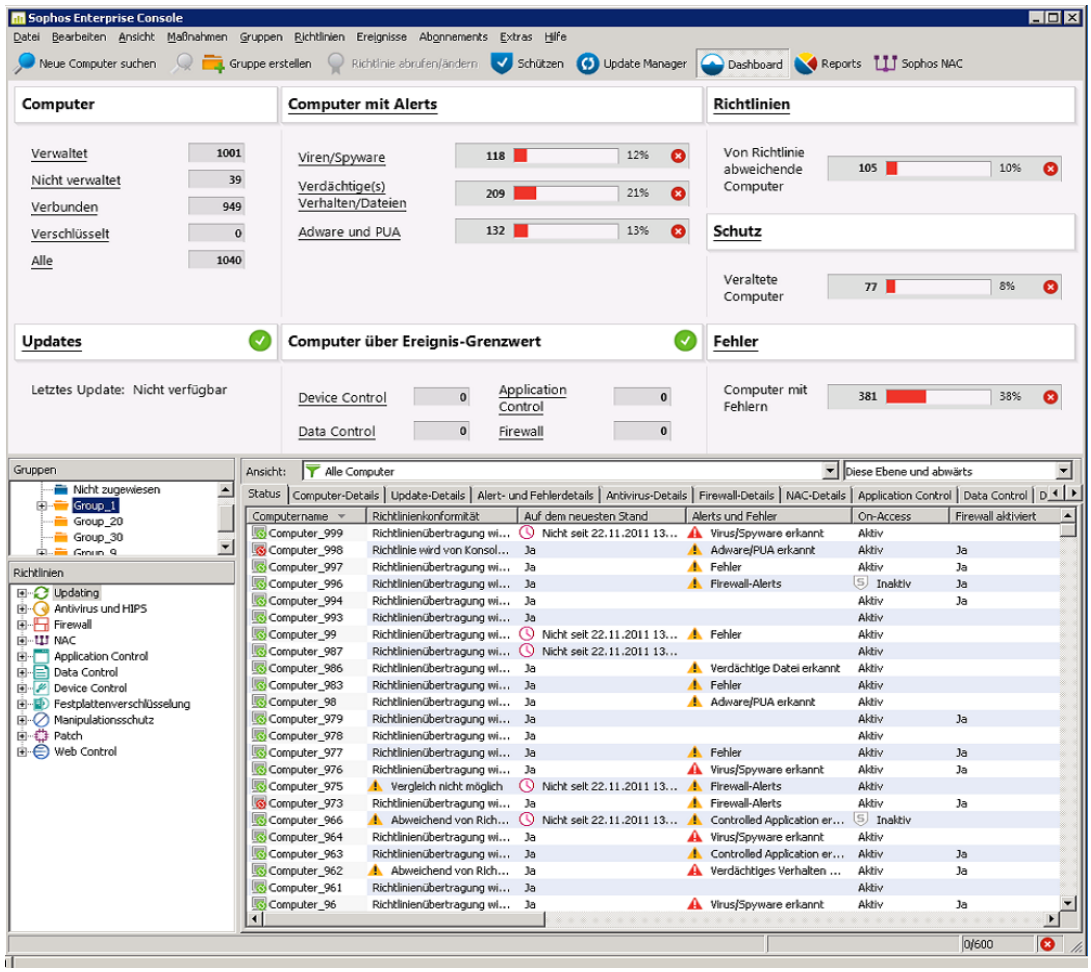
Weitere Informationen finden Sie unter *Dashboard-Bereiche* (Seite 7).

Computerliste

Die Computerliste befindet sich oben rechts. Sie bietet zwei Ansichten:

- In der **Ansicht „Endpoints“** werden die Endpoints der Gruppe angezeigt, die im Feld **Gruppen** unten links ausgewählt ist. Weitere Informationen finden Sie unter *Navigation in der Ansicht „Endpoints“* (Seite 9).
- Auf der Registerkarte **Update Manager** werden die Computer angezeigt, auf denen Sophos Update Manager installiert ist. Weitere Informationen finden Sie unter *Navigation in der Ansicht „Update Manager“* (Seite 13).

Der Screenshot unten zeigt die Computerliste in der Ansicht **Endpoints**.



2.2 Schaltflächen der Symbolleiste

Die folgende Tabelle bietet eine Übersicht über die Schaltflächen der Symbolleiste. Manche Schaltflächen sind nur unter bestimmten Umständen verfügbar. Die Schaltfläche **Schützen** zur Installation von Virenschutz- und Firewallsoftware ist etwa nur dann verfügbar, wenn eine Computergruppe im Feld **Gruppen** in der Ansicht **Endpoints** ausgewählt wurde.

Schaltflächen der Symbolleiste	Beschreibung
Ermitteln von Computern	Suche nach Computern im Netzwerk und Hinzufügen der Computer zur Konsole. Nähere Informationen entnehmen Sie bitte dem Abschnitt *Auswahl der Methode zur Ermittlung von Computern* (Seite 38) und anderen Themen im Bereich „*Einrichtung von Enterprise Console > Computersuche im Netzwerk*“.
Gruppen erstellen	Erstellen einer neuen Gruppe für Computer. Weitere Informationen finden Sie unter *Erstellen einer Gruppe* (Seite 29).

Schaltflächen der Symbolleiste	Beschreibung
Richtlinie öffnen/ändern	Öffnen der im Feld **Richtlinie** ausgewählten Richtline zum Ändern. Weitere Informationen finden Sie unter *Ändern einer Richtlinie* (Seite 36).
Schützen	Installieren der Virenschutz- und Firewallsoftware auf den in der Computerliste ausgewählten Computern. Weitere Informationen finden Sie unter *Automatisches Schützen von Computern* (Seite 51).
Endpoints	Wechsel in die Ansicht **Endpoints** in der Computerliste. Die Ansicht **Endpoints** zeigt die Computer der im Feld **Gruppe** ausgewählten Gruppe an. Weitere Informationen finden Sie unter *Navigation in der Ansicht „Endpoints“* (Seite 9).
Update Manager	Wechsel in die Ansicht **Update Manager** in der Computerliste. Auf der Registerkarte **Update Manager** werden die Computer angezeigt, auf denen Sophos Update Manager installiert ist. Weitere Informationen finden Sie unter *Navigation in der Ansicht „Update Manager“* (Seite 13).
Reports	Starten des **Report-Managers** zur Report-Erstellung zu Meldungen und Ereignissen im Netzwerk. Nähere Informationen finden Sie im Abschnitt *Reports* (Seite 223) und anderen Themen im Bereich „*Erstellen von Reports*“.
Dashboard	Anzeigen/Ausblenden des **Dashboards**. Das **Dashboard** zeigt den Sicherheitsstatus des Netzwerks auf einen Blick an. Weitere Informationen finden Sie unter *Dashboard-Bereiche* (Seite 7).
Sophos NAC	Öffnen von **Sophos NAC Manager**, damit Sie NAC-Richtlinien ändern können. Weitere Informationen finden Sie unter *Starten von NAC Manager* (Seite 151).

2.3 Dashboard-Bereiche

Das **Dashboard** umfasst folgende Bereiche:

Dashboard-Bereich	Beschreibung
Computer	Anzeige der Gesamtanzahl der Computer im Netzwerk sowie der Anzahl verbundener, verwalteter, nicht verwalteter und verschlüsselter Computer. Klicken Sie zum Anzeigen einer Liste verwalteter, nicht verwalteter, verbundener, verschlüsselter oder aller Computer auf einen der Links im Bereich **Computer**.
Updates	Anzeige des Status des Update Managers.
Computer mit Alerts	Anzeige der Anzahl und des prozentualen Anteils verwalteter Computer mit Alerts über Folgendes: ■ Bekannte und unbekannte Viren und Spyware ■ Verdächtiges Verhalten und verdächtige Dateien ■ Adware und andere potenziell unerwünschte Anwendungen Klicken Sie zum Aufrufen einer Liste verwalteter Computer mit ausstehenden Alerts auf den Bereichstitel **Computer mit Alerts**.
Computer über Ereignis-Grenzwert	Anzeige der Anzahl der Computer, auf denen die Summe der Ereignisse in den vergangenen 7 Tagen den angegebenen Höchstwert überschritten hat. Klicken Sie auf den jeweiligen Link im Abschnitt **Computer über Ereignis-Grenzwert**, um eine Liste der Computer mit Device Control-, Data Control-, Controlled Application- oder Firewall-Ereignissen aufzurufen.
Richtlinien	Anzeige der Anzahl und des prozentualen Anteils verwalteter Computer mit Verstößen gegen Gruppenrichtlinien oder Richtlinienabgleichsfehlern.

Dashboard-Bereich	Beschreibung
	Dazu gehören auch Computer, die noch nicht auf die geänderte Richtlinie reagiert haben, die ihnen von der Konsole gesendet wurde. Klicken Sie zur Anzeige einer Liste verwalteter Computer, die von der Richtlinie abweichen, auf **Richtlinien**.
Schutz	Anzeige der Anzahl und des prozentualen Anteils verwalteter und verbundener Computer, auf denen Sophos Endpoint Security and Control oder Sophos Anti-Virus nicht aktuell sind oder die unbekannte Erkennungsdaten verwenden. Klicken Sie zur Anzeige einer Liste verwalteter Computer, die sich nicht auf dem neuesten Stand befinden, auf **Schutz**.
Fehler	Anzeige der Anzahl und des prozentualen Anteils verwalteter Computer mit ausstehenden Scans, Updates oder Firewall-Fehlern. Klicken Sie zur Anzeige einer Liste verwalteter Computer mit ausstehenden Sophos Produktfehlern auf **Fehler**.

2.4 Sicherheitsstatussymbole

Die folgende Tabelle bietet eine Übersicht über die Sicherheitsstatussymbole im **Dashboard** sowie der Statusleiste von Enterprise Console.

Sicherheitsstatussymbol	Beschreibung
	Normal Die Anzahl betroffener Computer liegt unter der Warnstufe.
	Hinweis Der Warnschwellenwert wurde überschritten.
	Kritisch Der kritische Schwellenwert wurde überschritten.

Systemintegritätssymbole im Dashboard

Systemintegritätssymbole im **Dashboard** befinden sich jeweils in der rechten oberen Ecke eines Dashboard-Felds. Die Symbole zeigen den Status des jeweiligen Sicherheitsbereichs des Felds an.

Ein Statussymbol zur Systemintegrität im**Dashboard** zeigt den Status des Bereichs mit dem schwerwiegendsten Status an, d.h.:

- Ein Statussymbol des Bereichs ändert sich von **„Normal“** in **„Warnung“**, wenn ein Warnschwellenwert für mindestens ein Symbol in dem Bereich überschritten wird.

- Ein Statussymbol des Bereichs ändert sich von **„Warnung“** in **„Kritisch“**, wenn ein kritischer Schwellenwert für mindestens eine Anzeige in dem Bereich überschritten wird.

Symbol der Netzwerkintegrität

Das Symbol der Netzwerkintegrität wird auf der rechten Seite der Statusleiste von Enterprise Console angezeigt. Das Symbol gibt Aufschluss über den allgemeinen Sicherheitsstatus des Netzwerks.

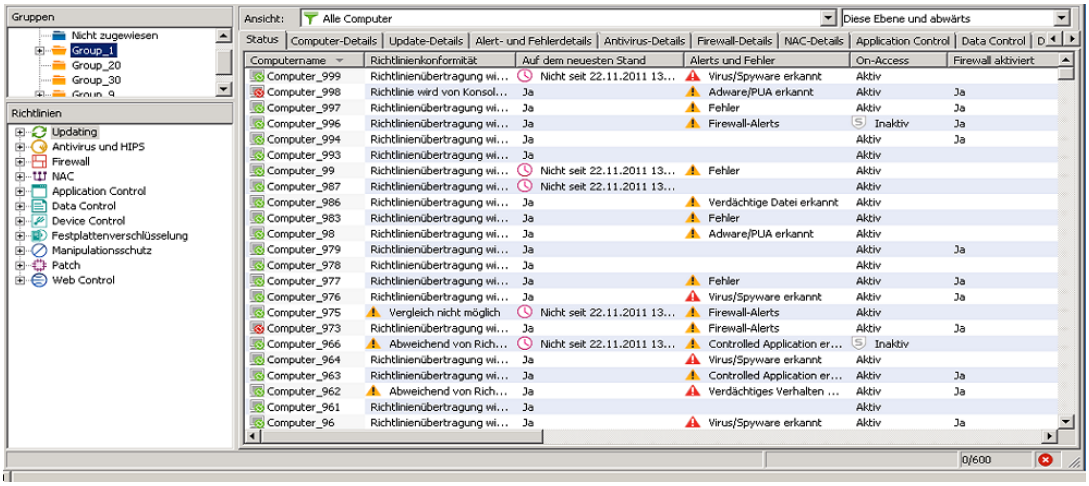
Das Statussymbol zur Netzwerkintegrität zeigt den Status des **Dashboard**-Bereichs mit dem schwerwiegendsten Status an, d.h.:

- Das Statussymbol zur Netzwerkintegrität ändert sich von **„Normal“** in **„Warnung“**, wenn ein Warnschwellenwert für mindestens eine Anzeige im Dashboard überschritten wird.
- Das Statussymbol zur Netzwerkintegrität ändert sich von **„Warnung“** in **„Kritisch“**, wenn ein kritischer Schwellenwert für mindestens eine Anzeige im **Dashboard** überschritten wird.

Bei der Erstinstallation oder einem Upgrade von Enterprise Console übernimmt das **Dashboard** die Standardwarnstufen und kritischen Stufen. Anweisungen zum Festlegen Ihrer eigenen Warnstufen und kritischen Stufen finden Sie unter *Konfigurieren des Dashboards* (Seite 56).

Sie können außerdem E-Mail-Benachrichtigungen einrichten, die an ausgewählte Empfänger gesendet werden sollen, wenn eine Warnstufe oder eine kritische Stufe für einen **Dashboard**-Bereich überschritten wird. Anweisungen hierzu finden Sie unter *Einrichten von Netzwerkstatus-E-Mail-Benachrichtigungen* (Seite 209).

2.5 Navigation in der Ansicht „Endpoints“



Computerliste

In der **Ansicht „Endpoints“** werden in der Computerliste die Endpoints der Gruppe angezeigt, die im Feld **Gruppen** ausgewählt ist.

Die Ansicht umfasst diverse Registerkarten. Aus der Registerkarte **Status** geht hervor, bei welchen Computern On-Access-Scans aktiviert sind, ob die Computer mit den Gruppenrichtlinien konform sind, welche Funktionen aktiviert sind und ob sich die Software

auf dem neuesten Stand befindet. Außerdem werden hier ggf. Alerts angezeigt. Auf den anderen Registerkarten finden Sie weitere Details zu den genannten Themen.

Sie können die Computerliste über den Filter **Ansicht** filtern. Wählen Sie im Dropdown-Menü **Ansicht** die Computer aus, die angezeigt werden sollen. So können Sie beispielsweise über die Option **Computer mit potenziellen Problemen** problematische Computer anzeigen lassen.

Sie können Computer nach Namen, Beschreibung oder IP-Adresse suchen. Weitere Informationen finden Sie unter *Computersuche in Enterprise Console* (Seite 12).

Die Symbole in der Computerliste werden im Abschnitt *Computerlistensymbole* (Seite 10) erläutert.

Sie können die Informationen der Computerliste in der Ansicht „Endpoints“ kopieren oder ausdrucken. Mehr dazu erfahren Sie unter *Kopieren von Daten aus der Computerliste* (Seite 238) und anderen Bereichen im Abschnitt *„Kopieren und Drucken von Daten mit Enterprise Console“*.

Der Fensterbereich „Gruppen“

Im Fensterbereich **Gruppen** können Sie Gruppen erstellen und Netzwerkcomputer in die Gruppen stellen. Sie können selbst Gruppen erstellen oder Active Directory-Container mit oder ohne Computer importieren und als Enterprise Console-Computergruppen einsetzen.

Nähere Informationen finden Sie im Abschnitt *Wofür gibt es Gruppen?* (Seite 28) und anderen Bereichen im Abschnitt *„Einrichtung von Enterprise Console“ > „Erstellen und Verwenden von Gruppen“*.

In der Gruppe **Nicht zugewiesen** befinden sich Computer, die noch keiner von Ihnen erstellten Gruppe zugeordnet wurden.

Fensterbereich „Richtlinien“

Im Fensterbereich **Richtlinien** erstellen und konfigurieren Sie die Richtlinien, die auf Computergruppen übertragen werden. Weitere Informationen finden Sie unter:

- *Informationen zu Richtlinien* (Seite 31) und anderen Bereichen im Abschnitt *„Einrichtung von Enterprise Console“ > „Erstellen und Verwenden von Gruppen“*
- Abschnitt *„Konfigurieren von Richtlinien“*

2.6 Computerlistensymbole

Alerts

Symbol	Erklärung
	Ein rotes Warnsymbol auf der Registerkarte **Status** in der Spalte **Alerts und Fehler** deutet darauf hin, dass ein Virus, Wurm, Trojaner, Spyware oder verdächtiges Verhalten erkannt wurde.

Symbol	Erklärung
	Ein gelbes Warnsymbol auf der Registerkarte **Status** in der Spalte **Alerts und Fehler** deutet auf eins der folgenden Probleme hin: ■ Eine verdächtige Datei wurde erkannt. ■ Adware oder eine andere potenziell unerwünschte Anwendung wurde erkannt. ■ Ein Fehler ist aufgetreten. Ein gelbes Warnsymbol in der Spalte **Richtlinienkonformität** weist darauf hin, dass die Richtlinie(n) des Computers von den anderen Computern der Gruppe abweichen.

Wenn für einen Computer mehrere Alerts oder Fehler vorhanden sind, wird in der Spalte **Alerts und Fehler** das Symbol des Alerts mit der höchsten Priorität angezeigt. Nachfolgend werden Alert-Typen nach Priorität in absteigender Reihenfolge aufgelistet.

1. Virus-/Spyware-Alert
2. Alerts bei verdächtigem Verhalten
3. Alerts bei verdächtigen Dateien
4. Adware-/PUA-Alerts
5. Software-Anwendungsfehler (beispielsweise Installationsfehler)

Schutz deaktiviert oder nicht aktuell

Ein graues Symbol in der Statusleiste der Komponenten auf der Registerkarte **Status** weist darauf hin, dass eine Funktion deaktiviert wurde. So weist etwa ein graues Schildsymbol ( ) in der Spalte **On-Access-Scans** darauf hin, dass On-Access-Scans deaktiviert wurden.

Ein Uhrensymbol in der Spalte **Auf dem neusten Stand** zeigt an, dass sich die Software nicht auf dem neuesten Stand befindet.

Computerstatus

Symbol	Erklärung
	Ein Computer-Symbol mit einem grünen Anschluss bedeutet, dass der Computer mit Enterprise Console verwaltet wird.
	Ein Computer-Symbol mit einer gelben Sanduhr bedeutet, dass die Installation von Sicherheitssoftware aussteht.
	Ein Computer-Symbol mit einem gelben, nach unten zeigenden Pfeil bedeutet, dass gerade Sicherheitssoftware installiert wird.
	Ein graues Computer-Symbol bedeutet, dass der Computer nicht von Enterprise Console verwaltet wird.

Symbol	Erklärung
	Ein Computersymbol mit einem roten Kreuz weist darauf hin, dass ein Computer, der von Enterprise Console verwaltet wird, nicht mit dem Netzwerk verbunden ist. (Nicht verwaltete Computer, die nicht mit dem Netzwerk verbunden sind, werden nicht angezeigt.)

2.7 Computersuche in Enterprise Console

In Enterprise Console können Sie anhand folgender Kriterien nach Computern suchen:

- Computername
- Computerbeschreibung
- IP-Adresse

1. Sie können anhand einer der folgenden Methoden nach Computern suchen:
   - Drücken Sie auf Strg. + F.
   - Klicken Sie im Menü **Bearbeiten** auf die Option **Computersuche**.
   - Klicken Sie an eine beliebige Stelle in der Computerliste, rechtsklicken Sie darauf und klicken Sie anschließend auf **Computersuche**.

2. Geben Sie die Suchkriterien ins **Suchfeld** ein.

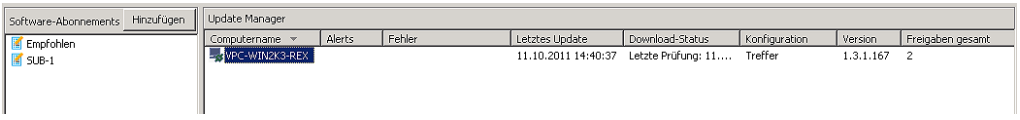
   Beim Feld **Suchen nach:** muss die Groß- und Kleinschreibung nicht beachtet werden. Platzhalter am Ende sind implizit.

   Sie können die Platzhalter * und ? benutzen.

   Beispiel:

Suchkriterien	Suchergebnisse
UKlapt	Sucht nach Zeichenfolgen, die mit „uklapt“ beginnen, z.B. „UKlaptop-011“, „UKlaptop-155“, „uklaptop132.
Ukla*	Sucht nach Zeichenfolgen, die mit „ukla“ beginnen. Der Platzhalter ist also nicht erforderlich, da die Suchergebnisse identisch sind (im Beispiel oben: „UKlaptop-011, UKlaptop-155, uklaptop132“).
***ukla**	Sucht nach Zeichenfolgen mit „ukla“, z.B. „UKlaptop-011“, „055uklax“, „056-Dukla-sales“.
Ukl*t	Sucht nach Zeichenfolgen, die mit „ukl“ beginnen, ein „t“ enthalten und mit einem beliebigen Zeichen aufhören, z.B. „UKlaptop-011“, „ukLite55“.
?klap	Sucht nach Zeichenfolgen, die mit einem beliebigen einzelnen Zeichen beginnen, ein „t“ enthalten und mit einem beliebigen Zeichen aufhören, z.B. „UKlaptop-011“, „ukLite55“ „uklapland33“.
UKl??t	Sucht nach Zeichenfolgen, die mit einem beliebigen einzelnen Zeichen beginnen, auf die ein „t“ folgt und die mit einem beliebigen Zeichen aufhören, z.B. „UKlaptop-011“, „uklist101“.

2.8 Navigation in der Ansicht „Update Manager“



Computerliste

In der Ansicht **Update Manager** können Sie automatische Updates für Sophos Sicherheitssoftware von der Sophos Website einrichten und den Status sowie weitere Informationen zu den Update Managern aufrufen.

In der Computerliste werden die Computer angezeigt, auf denen Sophos Update Manager installiert ist.

Software-Abonnements

Im Fensterbereich **Software-Abonnements** können Sie Software-Abonnements erstellen oder ändern und so angeben, welche Versionen der Endpoint-Software für das jeweilige System von Sophos heruntergeladen werden.

3 Erste Schritte mit Sophos Enterprise Console

Im Folgenden werden die Schritte zusammengefasst, die Sie nach der Installation von Enterprise Console und dem Ausführen des **Download-Assistenten für Sicherheitssoftware** durchführen müssen, um Ihr Netzwerk zu schützen. Nähere Informationen zu Enterprise Console finden Sie im Begleitmaterial und den genannten Abschnitten.

Praxistipps zum Einsatz und zur Verwaltung von Sophos Sicherheitssoftware finden Sie in der *Richtlinienanleitung* zu Sophos Enterprise Console. Sophos Begleitmaterial steht unter *http://www.sophos.de/support/docs/* zum Download bereit.

Wenn Sie den **Download-Assistenten für Sicherheitssoftware** nicht ausgeführt haben, lesen Sie den Abschnitt *Ausführen des Download-Assistenten für Sicherheitssoftware* (Seite 82).

Verfahren Sie wie folgt, um Ihr Netzwerk zu schützen:

1. Erstellen Sie Gruppen.

   Sie können selbst Gruppen erstellen oder Gruppen aus Active Directory-Containern mit oder ohne Computer importieren und als Enterprise Console Computer-Gruppen einsetzen.

   Anweisungen zum Importieren von Active Directory-Containern finden Sie unter *Importieren von Containern und Computern aus Active Directory* (Seite 38). Es empfiehlt sich, Active Directory-Container zunächst ohne Computer zu importieren, den Gruppen dann Gruppenrichtlinien zuzuweisen und Computer in die Gruppen (z.B. durch Synchronisieren der Gruppen mit Active Directory) aufzunehmen.

   Nähere Informationen zur manuellen Erstellung von Gruppen finden Sie unter *Wofür gibt es Gruppen?* (Seite 28) sowie an anderen Stellen im Unterabschnitt „*Erstellen und Einsatz von Gruppen*“ des Kapitels „*Einrichten von Enterprise Console* “.

2. Erstellen/Konfigurieren Sie Richtlinien.

   Enterprise Console bietet diverse Standardrichtlinien, die für den Netzwerkschutz unerlässlich sind. Die Standard-**Update**- und **Antivirus- und HIPS**-Richtlinie können Sie ohne Vornahme weiterer Einstellungen übernehmen. Führen Sie zum Konfigurieren der Firewall mit den **Firewall-Richtlinienassistenten** aus. Mehr dazu erfahren Sie unter *Einrichten einer Firewall-Richtlinie* (Seite 116).

3. Ermitteln Sie Computer im Netzwerk und fügen Sie sie zur Konsole hinzu.

   Wenn Sie bereits in Schritt 1 Container und Computer aus Active Directory importiert haben, können Sie diesen Schritt überspringen. Wenn nicht, ziehen Sie *Auswahl der Methode zur Ermittlung von Computern* (Seite 38) und andere Stellen im Unterabschnitt „Ermitteln von Computern im Netzwerk“ des Kapitels „*Einrichten von Enterprise Console* “ zu Rate.

4. Schützen Sie die Computer.

   Sie können zwischen zwei Methoden zum Schutz Ihrer Computer im Netzwerk wählen:

   - **Assistent zum Schutz für Computer**

     Wenn Sie einen Computer aus der Gruppe **Nicht zugewiesen** in eine andere Gruppe ziehen, wird ein Assistent gestartet, mit dessen Hilfe Sie die Computer schützen können. Nähere Informationen finden Sie unter *Automatisches Schützen von Computern* (Seite 51) und anderen Bereichen des Abschnitts „*Schützen von Computern*“.

   - **Automatischer Schutz von Computern bei der Synchronisierung mit Active Directory**

     Wenn Sie mit Active Directory synchronisieren möchten, können Sie auch Ihre Computer mit Windows 2000 und höher automatisch schützen. Dies stellen Sie im **Assistenten zur Synchronisierung mit Active Directory** oder im Dialogfeld **Synchronisierungseigenschaften** ein. Anweisungen hierzu finden Sie unter *Automatisches Schützen von Computern über Synchronisierung* (Seite 46).

5. Überprüfen Sie, ob die Computer geschützt sind.

   Wenn die Installation abgeschlossen ist, sehen Sie sich noch einmal die Computerliste in der neuen Gruppe an. In der Spalte **On-Access** sollte das Wort „*Aktiv*“ zu sehen sein, was darauf hinweist, dass der Computer durch On-Access-Scans geschützt ist und nun durch Enterprise Console gesteuert wird. Weitere Informationen finden Sie unter *So überprüfen Sie, ob Ihr Netzwerk geschützt ist* (Seite 56).

6. Führen Sie eine Bereinigung der Computer durch.

   Wenn ein Virus, ein sonstiges Objekt oder eine unerwünschte Anwendung im Netzwerk erkannt wird, bereinigen Sie die betroffenen Computer anhand der Anweisungen im Abschnitt *Sofortiges Bereinigen von Computern* (Seite 64).

Weitere Schutzoptionen

Standardmäßig erkennt Sophos Endpoint Security and Control Viren, Trojaner, Würmer und Spyware und analysiert das Verhalten der Programme, die auf dem System ausgeführt werden. Sie können weitere Schutzmechanismen hinzufügen, z.B. Schutz vor Adware, potenziell unerwünschten Anwendungen (PUA), verdächtigem oder unerwünschtem Verhalten oder ungewollten Datenverlusten über Computer. Weitere Informationen finden Sie in den folgenden Abschnitten:

- *Scannen auf verdächtige Dateien im Rahmen von On-Access-Scans* (Seite 102)
- *Scannen auf Adware und PUA* (Seite 96)
- *Was ist Application Control?* (Seite 153)
- *NAC* (Seite 150)
- *Informationen zur Patch-Analyse* (Seite 190)
- *Data Control* (Seite 156)
- *Device Control* (Seite 171)
- *Allgemeine Informationen* (Seite 187)

Verschlüsselungsoptionen

Wenn Verschlüsselung in Ihrem Lizenzumfang enthalten ist, können Sie Ihre Computer vor unbefugten Zugriffen schützen. Laufwerke können transparent verschlüsselt werden. Die POA (Power-on Authentication) stellt einen weiteren Authentifizierungsschritt vor dem Starten des Betriebssystems dar.

Verwaltungsoptionen

In Enterprise Console können Sie verschiedene *Rollen* erstellen und diesen Rechte und Windows-Benutzer und -Gruppen zuweisen. Die Rolle „Systemadministrator“, zu der auch die Windows-Gruppe „Sophos Full Administrators“ zählt, besitzt uneingeschränkte Zugriffsrechte und muss nicht eigens eingerichtet werden. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können Ihre IT-Verwaltungseinheit in *Teilverwaltungseinheiten* aufgliedern und den Teilverwaltungseinheiten Enterprise Console-Computergruppen zuweisen. Sie können den Zugriff auf die Teilverwaltungseinheiten regeln, indem Sie ihnen Windows-Benutzer und -Gruppen zuweisen. Die Teilverwaltungseinheit **Standard** umfasst alle Enterprise Console-Gruppen und die Gruppe **Nicht zugewiesen**. Nähere Informationen zu Teilverwaltungseinheiten finden Sie im Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 17).

4 Einrichtung von Enterprise Console

4.1 Verwalten von Rollen und Teilverwaltungseinheiten

4.1.1 Rollen und Teilverwaltungseinheiten

Wichtig: Wenn Sie bereits mit rollenbasierter Verwaltung arbeiten, müssen Sie zum Einrichten von Rollen und Teilverwaltungseinheiten über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Die Rolle „Systemadministrator“, zu der auch die Windows-Gruppe „Sophos Full Administrators“ zählt, besitzt uneingeschränkte Zugriffsrechte und muss nicht eigens eingerichtet werden. Mehr dazu erfahren Sie unter *Vordefinierte Rollen* (Seite 18) und *Aufgabenbereich der Berechtigungen* (Seite 22).

Wenn Sie rollenbasierten Zugriff zur Konsole einrichten möchten, können Sie Rollen erstellen, ihnen Rechte zuweisen und ihnen Windows-Benutzer und -Gruppen zuteilen. Zum Beispiel kann ein Helpdesk-Techniker Computer updaten und bereinigen, jedoch keine Richtlinien konfigurieren, da dies die Aufgabe eines Administrators ist.

Zum Öffnen von Enterprise Console muss ein Benutzer der Gruppe „Sophos Console Administrators“ angehören und mindestens einer Enterprise Console-Rolle und -Teilverwaltungseinheit zugewiesen worden sein. Mitglieder der Gruppe „Sophos Full Administrators“ besitzen uneingeschränkten Zugriff auf Enterprise Console.

Hinweis: Nähere Informationen zum Gewähren des Zugriffs auf eine Remote- oder weitere Instanz von Enterprise Console finden Sie unter *Wie kann ein anderer Anwender Enterprise Console nutzen?* (Seite 27).

Sie können selbst Rollen erstellen oder die Voreinstellungen übernehmen.

Benutzer können beliebig viele Rollen erhalten: Weisen Sie die Rolle dem Benutzer oder einer Windows-Gruppe zu, der er angehört.

Wenn ein Benutzer eine bestimmte Aufgabe von der Konsole aus nicht ausführen darf, kann er dennoch die entsprechenden Konfigurationseinstellungen aufrufen. Benutzer, denen keine Rollen zugewiesen wurden, können Enterprise Console nicht öffnen.

Sie können außerdem die Computer und Gruppen beschränken, auf die Benutzer zugreifen können. Sie können Ihre IT-Verwaltungseinheit in Teilverwaltungseinheiten aufgliedern und den Teilverwaltungseinheiten Enterprise Console-Computergruppen zuweisen. Sie können den Zugriff auf die Teilverwaltungseinheiten regeln, indem Sie ihnen Windows-Benutzer und -Gruppen zuweisen. Die Teilverwaltungseinheit **Standard** umfasst alle Enterprise Console-Gruppen und die Gruppe **Nicht zugewiesen**.

Benutzer können nur die Teilverwaltungseinheiten aufrufen, wenn sie ihnen zugewiesen wurden. Benutzer, die mehreren Teilverwaltungseinheiten zugewiesen wurden, können bestimmen, welche Teilverwaltungseinheit angezeigt werden soll. Es kann jeweils nur eine Teilverwaltungseinheit aufgerufen werden. Die in Enterprise Console geöffnete Teilverwaltungseinheit wird als *aktive Teilverwaltungseinheit* bezeichnet. Benutzer können keine Änderungen an Richtlinien vornehmen, die sich nicht in ihrer aktiven Teilverwaltungseinheit befinden.

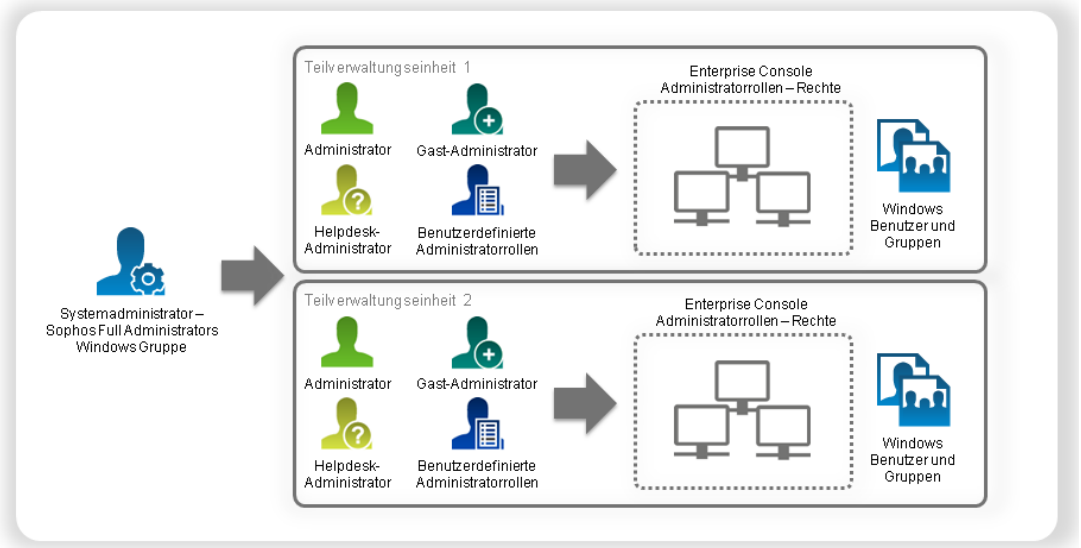


Abbildung 1: Rollen und Teilverwaltungseinheiten

4.1.2 Vordefinierte Rollen

Enterprise Console bietet vier vordefinierte Rollen:

Rolle	Beschreibung
Systemadministrator	Eine vorkonfigurierte Rolle für die Verwaltung von Sophos Sicherheitssoftware im Netzwerk und Rollen in Enterprise Console. Sie können die Rolle „Systemadministrator“ nicht modifizieren oder löschen.
Administrator	Eine vorkonfigurierte Berechtigungsklasse für die Verwaltung von Sophos Sicherheitssoftware im Netzwerk, jedoch nicht zur Verwaltung von Berechtigungsklassen in Enterprise Console. Sie können der Rolle „Administrator“ einen neuen Namen geben, die Rolle modifizieren oder löschen.
Helpdesk	Eine vorkonfigurierte Berechtigungsklasse, die nur über Korrekturrechte verfügt, z.B. zum Bereinigen oder Aktualisieren von Computern. Sie können die Rolle „Helpdesk“ umbenennen, modifizieren und löschen.
Gast	Eine vorkonfigurierte Berechtigungsklasse mit Lesezugriff auf Enterprise Console. Sie können die Rolle „Gast“ umbenennen, modifizieren und löschen.

Sie können die Rollen „Administrator“, „Helpdesk“ und „Gast“ an Ihre Bedürfnisse anpassen oder anhand der Anweisungen im Abschnitt *Erstellen einer Rolle* (Seite 19) eigene Rollen erstellen.

4.1.3 Erstellen einer Rolle

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Rufen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** die Registerkarte **Rollen verwalten** auf und klicken Sie auf **Erstellen**.

   Das Dialogfeld **Rolle erstellen** wird angezeigt.

3. Geben Sie einen Namen für die Funktion in das Feld **Name** ein.
4. Wählen Sie im Fenster **Berechtigungen** die Berechtigung(en) aus, die der Funktion zugewiesen werden sollen und klicken Sie auf **Hinzufügen**.
5. Klicken Sie im Fenster **Benutzer und Gruppen** auf **Hinzufügen**.
6. Geben Sie in das Dialogfeld **Benutzer oder Gruppe auswählen** den Namen eines Windows-Benutzers oder einer -Gruppe ein, dem/der Sie die Rolle zuweisen möchten. Klicken Sie auf **OK**.

   Bei Bedarf können Sie der Rolle mehr Benutzer oder Gruppen zuweisen. Anweisungen hierzu finden Sie in Schritt 5 und 6.

4.1.4 Löschen einer Rolle

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Wählen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** auf der Registerkarte **Rollen verwalten** die zu löschende Funktion aus und klicken Sie auf **Löschen**.

   Hinweis: Sie können die vordefinierte Rolle „Systemadministrator“ nicht löschen.

4.1.5 Ändern einer Rolle

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Wählen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** auf der Registerkarte **Rollen verwalten** die gewünschte Rolle aus und klicken Sie auf **Ändern**.

   Das Dialogfeld **Rolle ändern** wird angezeigt.

3. Weisen Sie im Fenster **Berechtigungen** den Rollen Berechtigungen zu oder entfernen Sie vorhandene Berechtigungen.

4. Fügen Sie im Fenster **Benutzer und Gruppen** Windows-Benutzer und -Gruppen zu der Rolle hinzu oder löschen Sie vorhandene Benutzer oder Gruppen.

4.1.6 Zuweisen von Berechtigungen zu Rollen

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Wählen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** auf der Registerkarte **Rollen verwalten** die gewünschte Rolle aus und klicken Sie auf **Ändern**.

   Das Dialogfeld **Rolle ändern** wird angezeigt.

3. Wählen Sie im Fenster **Berechtigungen** aus der **Berechtigungsliste** eine Berechtigung aus und klicken Sie auf **Hinzufügen**.

4.1.7 Erstellen einer Teilverwaltungseinheit

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Rufen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** die Registerkarte **Teilverwaltungseinheiten verwalten** auf und klicken Sie auf **Erstellen**.

   Das Dialogfeld **Teilverwaltungseinheit erstellen** wird angezeigt.

3. Geben Sie einen Namen für die Teilverwaltungseinheit in das Feld **Name** ein.
4. Wählen Sie im Fenster **Enterprise Console-Gruppen** die Gruppen aus, die Sie in die Teilverwaltungseinheit aufnehmen möchten.
5. Klicken Sie im Fenster **Benutzer und Gruppen** auf **Hinzufügen**, um Windows-Benutzer und -Gruppen in die Teilverwaltungseinheit aufzunehmen.

4.1.8 Ändern der aktiven Teilverwaltungseinheit

Wenn Ihnen mehrere Teilverwaltungseinheiten zugewiesen wurden, können Sie festlegen, welche Teilverwaltungseinheiten beim Öffnen von Enterprise Console angezeigt werden und in Enterprise Console zu einer anderen Teilverwaltungseinheit wechseln.

Es kann jeweils nur eine Teilverwaltungseinheit angezeigt werden. Wenn Sie die aktive Teilverwaltungseinheit ändern, wird Enterprise Console mit der neuen Teilverwaltungseinheit neu geladen.

So können Sie die aktive Teilverwaltungseinheit ändern:

1. Klicken Sie im Menü **Extras** auf **Aktive Teilverwaltungseinheit auswählen**.

2. Wählen Sie im Dialogfeld **Aktive Teilverwaltungseinheit auswählen** die Teilverwaltungseinheit aus, die Sie öffnen möchten, und klicken Sie auf **OK**.

4.1.9 Ändern einer Teilverwaltungseinheit

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Wählen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** auf der Registerkarte **Teilverwaltungseinheiten verwalten** die zu ändernde Teilverwaltungseinheit aus und klicken Sie auf **Ändern**.
3. Im Dialogfeld **Teilverwaltungseinheit ändern** können Sie den Namen der Teilverwaltungseinheit, die Enterprise Console-Gruppen der Teilverwaltungseinheit und die Windows-Benutzer und -Gruppen ändern, die Zugriff auf die Teilverwaltungseinheit besitzen. Klicken Sie auf **OK**.

4.1.10 Kopieren einer Teilverwaltungseinheit

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Wählen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** auf der Registerkarte **Teilverwaltungseinheiten verwalten** die gewünschte Teilverwaltungseinheit aus und klicken Sie auf **Kopieren**.

   In der Liste der Teilverwaltungseinheiten erscheint nun eine Kopie der Teilverwaltungseinheit.

3. Wählen Sie die neue Teilverwaltungseinheit aus und klicken Sie auf **Ändern**. Benennen Sie die Teilverwaltungseinheit um. Auf Wunsch können Sie die Gruppen der Teilverwaltungseinheit sowie die Windows-Benutzer und -Gruppen ändern, die darauf zugreifen können.

4.1.11 Löschen einer Teilverwaltungseinheit

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Rollenbasierte Verwaltung** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Wählen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** auf der Registerkarte **Teilverwaltungseinheiten verwalten** die zu löschende Teilverwaltungseinheit aus und klicken Sie auf **Löschen**.

   Die **Standard**-Teilverwaltungseinheit kann nicht gelöscht werden.

4.1.12 Anzeigen von Rollen und Teilverwaltungseinheiten von Benutzern und Gruppen

So können Sie die Rollen und Teilverwaltungseinheiten von Windows-Benutzern und -Gruppen aufrufen:

1. Klicken Sie im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten verwalten**.
2. Rufen Sie im Dialogfeld **Rollen und Teilverwaltungseinheiten verwalten** die Registerkarte **Benutzer-/Gruppenansicht** auf und klicken Sie auf die Schaltfläche **Benutzer/Gruppe** auswählen.
3. Wählen Sie im Dialogfeld **Benutzer/Gruppe auswählen** einen Benutzer oder eine Gruppe aus, dessen/deren Rollen und Teilverwaltungseinheiten angezeigt werden sollen und klicken Sie auf **OK**.

4.1.13 Aufgabenbereich der Berechtigungen

Berechtigung	Tasks
Computersuche, -schutz und -gruppen	Suche starten, Suche anhalten und Suche nach Domänen (Netzwerksuche, IP-Bereichsuche und Active Directory-Suche)
	Importieren von Computern und Gruppen aus Active Directory, Importieren von Gruppen aus Active Directory
	Importieren von Computern aus einer Datei
	Löschen eines Computers
	Schützen eines Computers
	Synchronisierung von Gruppen mit Active Directory
	Ändern der Synchronisierungseigenschaften von Gruppen
	Gruppensynchronisierung entfernen
	Verschieben eines Computers
	Erstellen einer Gruppe
	Umbenennen einer Gruppe
	Verschieben einer Gruppe
	Löschen einer Gruppe
	Übertragen einer Richtlinie auf eine Gruppe
Anpassung von Data Control	Erstellen einer Data Control-Regel
	Ändern einer Data Control-Regel

Berechtigung	Tasks
	Kopieren einer Data Control-Regel
	Löschen einer Data Control-Regel
	Ausschließen von Dateien von Data Control-Scans
	Erstellen einer Content Control List
	Ändern einer Content Control List
	Kopieren einer Content Control List
	Löschen einer Content Control List
Data Control-Ereignisse	Anzeige der Data Control-Ereignisanzeige
	Anzeige von Data Control-Ereignissen in den Computerdetails
Richtlinieneinstellung – Antivirus und HIPS	Erstellen einer Antivirus- und HIPS-Richtlinie
	Duplizieren einer Antivirus- und HIPS-Richtlinie
	Umbenennen einer Antivirus- und HIPS-Richtlinie
	Ändern einer Antivirus- und HIPS-Richtlinie
	Wiederherstellen der Standardeinstellungen von Antivirus und HIPS
	Löschen einer Antivirus- und HIPS-Richtlinie
	Hinzufügen oder Entfernen von Einträgen aus einer Threat-Masterliste
Richtlinieneinstellung – Application Control	Erstellen einer Application Control-Richtlinie
	Duplizieren einer Application Control-Richtlinie
	Umbenennen einer Application Control-Richtlinie
	Ändern einer Application Control-Richtlinie
	Wiederherstellung der Standardeinstellungen von Application Control
	Löschen einer Application Control-Richtlinie
Richtlinieneinstellung – Data Control	Erstellen einer Data Control-Richtlinie
	Duplizieren einer Data Control-Richtlinie
	Umbenennen einer Data Control-Richtlinie
	Ändern einer Data Control-Richtlinie

Berechtigung	Tasks
	Wiederherstellen der Data Control-Einstellungen
	Löschen einer Data Control-Richtlinie
Richtlinieneinstellung – Device Control	Erstellen einer Device Control-Richtlinie
	Duplizieren einer Device Control-Richtlinie
	Umbenennen einer Device Control-Richtlinie
	Ändern einer Device Control-Richtlinie
	Wiederherstellen der Standardeinstellungen von Device Control
	Löschen einer Device Control-Richtlinie
Richtlinieneinstellung – Firewall	Erstellen einer Firewall-Richtlinie
	Duplizieren einer Firewall-Richtlinie
	Umbenennen einer Firewall-Richtlinie
	Ändern einer Firewall-Richtlinie
	Wiederherstellen der Standardeinstellungen der Firewall
	Löschen einer Firewall-Richtlinie
Richtlinieneinstellung – NAC	Anzeige einer NAC-Richtlinie
Richtlinieneinstellung – Patch	Erstellen einer Patch-Richtlinie
	Duplizieren einer Patch-Richtlinie
	Umbenennen einer Patch-Richtlinie
	Ändern einer Patch-Richtlinie
	Wiederherstellen der Standard-Patch-Einstellungen
	Löschen einer Patch-Richtlinie
Richtlinieneinstellung – Manipulationsschutz	Erstellen einer Manipulationsschutz-Richtlinie
	Duplizieren einer Manipulationsschutz-Richtlinie
	Umbenennen einer Manipulationsschutz-Richtlinie
	Bearbeiten einer Manipulationsschutz-Richtlinie
	Wiederherstellen der Standardeinstellungen des Manipulationsschutzes
	Löschen einer Manipulationsschutz-Richtlinie

Berechtigung	Tasks
Richtlinieneinstellung – Updates	Erstellen einer Update-Richtlinie
	Duplizieren einer Update-Richtlinie
	Umbenennen einer Update-Richtlinie
	Ändern einer Update-Richtlinie
	Wiederherstellen der Standard-Update-Einstellungen
	Löschen einer Update-Richtlinie
	Erstellen von Abonnements
	Ändern von Abonnements
	Umbenennen von Abonnements
	Duplizieren von Abonnements
	Löschen von Abonnements
	Konfigurieren von Update Managern
Richtlinieneinstellung - Web Control	Erstellen einer Web Control-Richtlinie
	Duplizieren einer Web Control-Richtlinie
	Umbenennen einer Web Control-Richtlinie
	Ändern einer Web Control-Richtlinie
	Zurücksetzen einer Web Control-Richtlinie
	Löschen einer Web Control-Richtlinie
Richtlinieneinstellung – Festplattenverschlüsselung	Erstellen einer Richtlinie zur Festplattenverschlüsselung
	Duplizieren einer Richtlinie zur Festplattenverschlüsselung
	Umbenennen einer Richtlinie zur Festplattenverschlüsselung
	Ändern einer Richtlinie zur Festplattenverschlüsselung
	Wiederherstellen der Standardeinstellungen der Festplattenverschlüsselung
	Löschen einer Richtlinie zur Festplattenverschlüsselung
Globale Verschlüsselungseinstellungen	Ändern der globalen Verschlüsselungseinstellungen
	Sichern von Unternehmenszertifikaten
	Sichern der Schlüssel-Recovery-Datei

Berechtigung	Tasks
Korrektur – Bereinigung	Bereinigung erkannter Objekte
	Alerts löschen
	Fehler löschen
Korrektur – Updates und Scans	Computer jetzt updaten
	Durchführen einer vollständigen Systemüberprüfung
	Durchsetzen von Gruppenrichtlinien
	Übernahme der Konfigurationseinstellungen
	Anweisung an den Update Manager, sofort ein Update durchzuführen
Korrektur – Verschlüsselungs-Recovery	Wiederherstellen des Zugriffs auf verschlüsselte Computer mit Challenge/Response
Report-Konfiguration	Erstellen, Bearbeiten und Löschen eines Reports
Rollenbasierte Verwaltung	Erstellen einer Rolle
	Umbenennen einer Rolle
	Löschen einer Rolle
	Ändern der Berechtigungen einer Rolle
	Hinzufügen von Benutzern/Gruppen zur Rolle
	Entfernen eines Benutzers/einer Gruppe von einer Funktion
	Verwalten von Teilverwaltungseinheiten: Erstellen einer Teilverwaltungseinheit; Umbenennen einer Teilverwaltungseinheit; Löschen einer Teilverwaltungseinheit; Hinzufügen einer Teilverwaltungseinheit; Entfernen einer Stammgruppe einer Teilverwaltungseinheit, Hinzufügen von Benutzern/Gruppen zu einer Teilverwaltungseinheit, Entfernen von Benutzern/Gruppen von einer Teilverwaltungseinheit
Systemkonfiguration	Ändern der SMTP-Servereinstellungen; Testen der SMTP-Servereinstellungen; Hinzufügen von Empfängern von E-Mail-Benachrichtigungen
	Konfigurieren der Warnstufen und kritischen Stufen für das Dashboard
	Konfigurieren von Reports: Konfigurieren der Datenbank-Alert-Bereinigung; Einstellen des in Reports angezeigten Firmennamens

Berechtigung	Tasks
	Konfigurieren von Reports an Sophos: Aktivieren/Deaktivieren der Benachrichtigungen an Sophos; Ändern des Benutzernamens; Ändern der Kontakt-E-Mail-Adresse
	Konfigurieren der NAC-URL
Web-Ereignisse	Anzeige der Web-Ereignisanzeige
	Anzeige von Web-Ereignissen in den Computerdetails

4.1.14 Wie kann ein anderer Anwender Enterprise Console nutzen?

Mitglieder der Gruppe „Sophos Full Administrators“ besitzen uneingeschränkten Zugriff auf Enterprise Console.

Sie können anderen Benutzern Zugriff auf Enterprise Console gewähren. Benutzer müssen zum Öffnen von Enterprise Console folgende Voraussetzungen erfüllen:

- Mitglied der Gruppe „Sophos Console Administrators“ sein.
- Mindestens eine Rolle in Enterprise Console wahrnehmen.
- Mindestens einer Teilverwaltungseinheit in Enterprise Console angehören.

Fügen Sie Benutzer mit Windows-Tools zu einer „Sophos Console Administrators“-Gruppe hinzu.

Klicken Sie zum Zuweisen eines Benutzers zu Rollen oder Teilverwaltungseinheiten in Enterprise Console im Menü **Extras** auf **Rollen und Teilverwaltungseinheiten**. Nähere Informationen zu Rollen und Teilverwaltungseinheiten finden Sie im Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 17).

Benutzer müssen zum Zugriff auf eine Remote- oder eine zusätzliche Instanz von Enterprise Console folgende Voraussetzungen erfüllen:

- Mitglied der Gruppe „Sophos Console Administrators“ auf dem Server sein, auf dem der Enterprise Console-Management-Server installiert ist.
- Mitglied der Gruppe „Distributed COM-Benutzer“ auf dem Server sein, auf dem der Enterprise Console-Management-Server installiert ist. (Die Gruppe „Distributed COM-Benutzer“ befindet sich im vordefinierten Container des Active Directory-Benutzer und -Computer-Tools.)
- Mindestens eine Rolle in Enterprise Console wahrnehmen.
- Mindestens einer Teilverwaltungseinheit in Enterprise Console angehören.

4.2 Erstellen und Einsatz von Gruppen

4.2.1 Wofür gibt es Gruppen?

Sie müssen Gruppen erstellen und ihnen Computer zuordnen, bevor Sie diese Computer schützen und verwalten können.

Gruppen bieten die folgenden Vorteile:

- Updaten von Computern in unterschiedlichen Gruppen von verschiedenen Quellen oder über verschiedene Zeitpläne.
- Einsatz unterschiedlicher Antivirus- und HIPS-, Application Control-, Firewall- oder sonstiger Richtlinien für die einzelnen Gruppen.
- Einfachere Computerverwaltung.

Tipp: Sie können Gruppen innerhalb von Gruppen erstellen und bestimmte Richtlinien auf jede Gruppe und Untergruppe übertragen.

4.2.2 Was ist eine Gruppe?

Eine Gruppe ist ein Ordner, der mehrere Computer enthält.

Sie können selbst Gruppen erstellen oder Active Directory-Container mit oder ohne Computer importieren und als Enterprise Console Computergruppen einsetzen. Sie können außerdem eine Synchronisierung mit Active Directory einstellen, damit neue Computer und Container sowie andere Änderungen in Active Directory automatisch auf Enterprise Console übertragen werden.

Jede Gruppe hat eigene Einstellungen für Updates, Viren- und HIPS-Schutz, Firewall-Schutz usw. Alle Computer einer Gruppe sollten normalerweise diese Einstellungen („Richtlinie“) verwenden.

Eine Gruppe kann Untergruppen enthalten.

4.2.3 Wozu dient die Gruppe „Nicht zugewiesen“?

Enterprise Console legt Computer vor der Einteilung in der Gruppe **Nicht zugewiesen** ab.

Sie können nicht:

- Richtlinien auf die Gruppe **Nicht zugewiesen** übertragen.
- In der Gruppe **Nicht zugewiesen** weitere Gruppen erstellen.
- Die Gruppe **Nicht zugewiesen** verschieben oder löschen.

4.2.4 Erstellen einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So können Sie eine neue Gruppe für Computer erstellen:

1. Wählen Sie in der Ansicht **Endpoints** im Fensterbereich **Gruppen** (links in der Konsole), wo Sie die Gruppe erstellen möchten.

   Klicken Sie auf den Computernamen oben, wenn Sie eine neue Top-Level-Gruppe erstellen möchten. Klicken Sie auf eine bestehende Gruppe, wenn Sie eine Untergruppe erstellen möchten.

2. Klicken Sie in der Symbolleiste auf das Symbol **Gruppe erstellen**.

   Eine „Neue Gruppe“ wird in die Liste aufgenommen. Der Name der Gruppe ist markiert.

3. Geben Sie einen Namen für die Gruppe ein.

Update-, Anti-Virus- und HIPS-, Application Control-, Firewall-, NAC- (Network Access Control), Patch-, Data Control-, Device Control, Manipulationsschutz- und Web Control-Richtlinien werden automatisch auf die neue Gruppe übertragen. Sie können diese Richtlinien ändern oder andere Richtlinien anwenden. Nähere Informationen finden Sie unter *Ändern einer Richtlinie* (Seite 36) und *Übertragen einer Richtlinie auf eine Gruppe* (Seite 36).

Hinweis: Wenn es sich bei der neuen Gruppe um eine Untergruppe handelt, verwendet die Untergruppe anfangs dieselben Einstellungen wie die Gruppe, in der sie sich befindet.

4.2.5 Zuweisen von Computern zu einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Markieren Sie die Computer, die Sie in eine Gruppe aufnehmen möchten. Klicken Sie z.B. auf die Gruppe **Nicht zugewiesen** und markieren Sie dort Computer.
2. Ziehen Sie die Computer mittels Drag-and-Drop in die neue Gruppe.

   Wenn Sie ungeschützte Computer aus der Gruppe **Nicht zugewiesen** in eine Gruppe verschieben, für die automatische Updates eingerichtet sind, wird ein Assistent gestartet, der Ihnen dabei hilft, diese Computer zu schützen.

   Wenn Sie Computer von einer Gruppe in eine andere verschieben, verwenden Sie die gleichen Richtlinien wie die Computer, die sich bereits in der Gruppe befinden, in die sie verschoben wurden.

4.2.6 Löschen von Computern aus einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können Computer aus einer Gruppe löschen, z.B. wenn Sie Einträge für Computer entfernen möchten, die sich nicht mehr im Netzwerk befinden.

Wichtig: Wenn Sie Computer löschen, die sich noch im Netzwerk befinden, werden sie nicht mehr in der Konsole aufgelistet oder von ihr verwaltet.

So löschen Sie Computer:

1. Markieren Sie die Computer, die Sie löschen möchten.
2. Rechtsklicken Sie auf die Auswahl und wählen Sie **Löschen**.

Wenn Sie die Computer erneut sehen möchten, klicken Sie in der Symbolleiste auf das Symbol **Computer ermitteln**. Die Computer werden bis zum nächsten Neustart nicht als verwaltet angezeigt.

4.2.7 Verschieben einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Markieren Sie die Gruppe, die Sie verschieben möchten. Klicken Sie im Menü **Bearbeiten** auf **Ausschneiden**.
2. Markieren Sie die Gruppe, in die Sie die Gruppe einfügen möchten. Klicken Sie im Menü **Bearbeiten** auf **Einfügen**.

4.2.8 Löschen einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Alle Computer, die sich in der gelöschten Gruppe befanden, werden in der Gruppe **Nicht zugewiesen** abgelegt.

1. Markieren Sie die Gruppe, die Sie löschen möchten.
2. Rechtsklicken Sie auf die Auswahl und wählen Sie **Löschen**. Bestätigen Sie bei entsprechender Aufforderung, dass Sie die Gruppe und gegebenenfalls deren Untergruppen löschen möchten.

4.2.9 Umbenennen einer Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Markieren Sie die Gruppe, die Sie umbenennen möchten.
2. Rechtsklicken Sie auf die Auswahl und wählen Sie **Umbenennen**.

4.2.10 Welche Richtlinien sind einer Gruppe zugewiesen?

So können Sie feststellen, welche Richtlinien einer Gruppe zugewiesen wurden:

- Rechtsklicken Sie im Fensterbereich **Gruppen** auf die Gruppe. Wählen Sie **Gruppenrichtliniendetails öffnen**.

  Im Dialogfeld „Gruppendetails“ können Sie die Richtlinien ansehen, die derzeit verwendet werden.

4.3 Erstellen und Einsatz von Richtlinien

4.3.1 Informationen zu Richtlinien

In einer Richtlinie werden Einstellungen zusammengefasst, die für alle Computer in einer Gruppe gelten.

- Die **Update**-Richtlinie gibt an, wie Computer mit neuer Sicherheitssoftware upgedatet werden.
- In der **Anti-Virus- und HIPS**-Richtlinie ist festgelegt, wie die Sicherheitssoftware Computer auf Viren, Trojaner, Würmer, Spyware, Adware, potenziell unerwünschte Anwendungen, verdächtige Dateien und Verhaltensmuster scannt und sie davon bereinigt.
- In der **Application Control**-Richtlinie ist festgelegt, welche Anwendungen auf Ihren Computern gesperrt und welche zugelassen sind.
- Die **Firewall**-Richtlinie gibt an, wie die Firewall Computer schützt.
- Die **Data Control**-Richtlinie umfasst Regeln zum Überwachen bzw. Beschränken von Dateiübertragungen auf der Basis des Inhalts, Namens und Typs von Dateien.
- In der **Device Control**-Richtlinie werden die Speichermedien und Netzwerkgeräte festgelegt, die nicht auf Arbeitsplatzrechnern verwendet werden dürfen.
- Die **NAC**-Richtlinie enthält die von Computern zu erfüllenden Bedingungen für den Netzwerkzugriff.
- In der **Patch**-Richtlinie wird festgelegt, ob die Patch-Analyse aktiviert ist und in welchem Intervall sie ggf. stattfinden soll.
- In der Richtlinie zur **Festplattenverschlüsselung** wird angegeben, wie Computer durch die Festplattenverschlüsselung vor nicht zulässigem Zugriff geschützt werden.
- Die **Manipulationsschutz**-Richtlinie umfasst das Kennwort, über das autorisierte Endpoint-Benutzer Sophos Sicherheitssoftware konfigurieren, deaktivieren oder deinstallieren können.
- In der **Web Control**-Richtlinie wird festgelegt, welche Websites Benutzer aufrufen können. Benutzer werden über Seiten benachrichtigt, die in die Kategorie „Blockieren“ oder „Warnen“ fallen.

Sie können mehr als eine Richtlinie von jedem Typ erstellen.

Sie können die gleiche Richtlinie auf mehr als eine Gruppe übertragen.

4.3.2 Was ist eine Richtlinie?

In einer Richtlinie werden Einstellungen zusammengefasst, die für alle Computer in einer Gruppe gelten.

Bei der Installation von Enterprise Console werden Standardrichtlinien erstellt, die für einen Basisschutz sorgen. Diese Richtlinien werden auf neu erstellte Gruppen übertragen. Sie können die Standardrichtlinien ändern oder neue Richtlinien erstellen.

Nähere Informationen über die unterschiedlichen Richtlinienarten finden Sie im Abschnitt *Informationen zu Richtlinien* (Seite 31).

4.3.3 Standardrichtlinien

Bei der Installation von Enterprise Console werden Standard-Richtlinien erstellt.

Update-Richtlinie

Die Standard-Update-Richtlinie bietet Folgendes:

- Automatische Updates der Computer alle zehn Minuten vom Standardverzeichnis. Das Standardverzeichnis lautet: UNC-Freigabe \\<Computername>\SophosUpdate. Dabei ist „Computername“ der Name des Computers, auf dem der Update Manager installiert ist.

Antivirus- und HIPS-Richtlinie

Die Standard-Antiviren- und HIPS-Richtlinie bietet Folgendes:

- On-Access-Scans auf Viren und Spyware (jedoch nicht verdächtige Dateien und Adware oder andere potenziell unerwünschte Anwendungen).
- Analyse der auf dem System laufenden Programme (Sophos Anti-Virus und Sophos Endpoint Security and Control für Windows 2000 und höher).
- Sicherheits-Alerts, die auf dem Desktop des betroffenen Computers angezeigt und zum Ereignisprotokoll hinzugefügt werden.

Application Control-Richtlinie

Standardmäßig werden alle Anwendungen und Anwendungstypen zugelassen. On-Access-Scans auf Anwendungen, die Sie eventuell überwachen möchten, sind nicht aktiviert.

Firewall-Richtlinie

Standardmäßig ist die Sophos Client Firewall aktiviert und sperrt unnötigen Datenfluss. Konfigurieren Sie die Firewall zunächst so, dass gewünschte Anwendungen zugelassen werden, bevor Sie sie im gesamten Netzwerk einsetzen. Mehr dazu erfahren Sie unter *Einrichten einer Firewall-Richtlinie* (Seite 116).

Eine vollständige Beschreibung der Firewall-Einstellungen ist dem Sophos Support-Artikel 57757 (*http://www.sophos.de/support/knowledgebase/article/57757.html*) zu entnehmen.

Data Control-Richtlinie

Standardmäßig ist Data Control deaktiviert und es sind keine Regeln zur Überwachung oder Einschränkung der Übertragung von Dateien auf das Internet oder auf Speichermedien festgelegt.

Device Control-Richtlinie

Device Control ist standardmäßig deaktiviert und alle Geräte sind zugelassen.

NAC-Richtlinie

Wenn Sie die Standardrichtlinie oder den „Richtlinien-Modus“ im NAC-Server nicht geändert haben, verfügen alle Computer über Netzwerkzugriffsrechte.

Patch-Richtlinie

Die Patch-Analyse ist standardmäßig deaktiviert. Bei neuen Patch-Richtlinien ist die Analyse aktiviert. Nach Aktivierung der Patch-Analyse werden die Computer täglich auf fehlende Patches analysiert, sofern kein anderes Intervall ausgewählt wurde.

Manipulationsschutz-Richtlinie

Standardmäßig ist der Manipulationsschutz deaktiviert und für die Konfiguration, Deaktivierung oder Deinstallation von Sophos Sicherheitssoftware ist kein Kennwort festgelegt.

Web Control-Richtlinie

Standardmäßig ist Web Control deaktiviert: Benutzer können alle Websites aufrufen, die nicht vom Web-Schutz von Enterprise Console blockiert werden. Mehr dazu erfahren Sie unter *Der Web-Schutz* (Seite 98).

Richtlinie zur Festplattenverschlüsselung

Standardmäßig werden Festplatten auf Computern nicht verschlüsselt. Wenn Sie zu verschlüsselnde Volumes in der Standardrichtlinie angeben, werden die ausgewählten Volumes auf Computerlaufwerken mit der schnellen Erstverschlüsselung verschlüsselt.

Hinweis: Wenn eine Festplatte vor der Verschlüsselung verwendet wurde, ist die schnelle Erstverschlüsselung unter Umständen unsicherer. Nicht verwendete Sektoren können noch Daten enthalten.

Zur Anmeldung ist die POA aktiviert. Zur Recovery ist Challenge/Response aktiviert und wird entsprechend konfiguriert.

4.3.4 Muss ich meine eigenen Richtlinien erstellen?

Bei der Installation von Enterprise Console werden Standardrichtlinien erstellt. Diese Richtlinien werden auf neu erstellte Gruppen übertragen.

Die Standardrichtlinien bieten Ihnen grundlegenden Schutz. Wenn Sie jedoch Funktionen wie Network Access Control oder Application Control nutzen möchten, müssen Sie neue Richtlinien erstellen oder zumindest die Standardrichtlinien ändern.

Hinweis: Wenn Sie die Standardrichtlinie ändern, wirken sich die Änderungen auf alle neu erstellten Richtlinien aus.

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Erstellen oder Ändern einer Richtlinie über die Berechtigung **Richtlinieneinstellung** verfügen. Wenn Sie beispielsweise eine Antivirus- und HIPS-Richtlinie erstellen oder ändern möchten, benötigen Sie die Berechtigung **Richtlinieneinstellung – Anti-Virus und HIPS**. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Update-Richtlinie

In der Standard-Update-Richtlinie ist festgelegt, dass alle zehn Minuten auf Updates des empfohlenen Abonnements von der Standard-UNC-Freigabe zur Softwareverteilung geprüft werden soll. Wenn Sie Abonnements, Update-Standorte oder sonstige Einstellungen ändern möchten, konfigurieren Sie Update-Richtlinien anhand der Anweisungen im Abschnitt *Update-Richtlinie* (Seite 82).

Antivirus und HIPS

Die Antivirus- und HIPS-Standardrichtlinie schützt Computer vor Viren und sonstiger Malware. Sie können aber auch neue Richtlinien erstellen oder die Standardrichtlinie ändern, um die Erkennung anderer unerwünschte/verdächtiger Anwendungen oder Verhaltensmuster zu ermöglichen. Mehr dazu erfahren Sie unter *Die Antivirus- und HIPS-Richtlinie* (Seite 94).

Application Control

Konfigurieren Sie zum Festlegen und Sperren nicht zulässiger Anwendungen Application Control-Richtlinien. Anweisungen hierzu finden Sie unter *Was ist Application Control?* (Seite 153).

Firewall-Richtlinie

Konfigurieren Sie Firewall-Richtlinien, um vertrauenswürdigen Anwendungen Netzwerkzugang zu gewähren. Anweisungen hierzu finden Sie unter *Einrichten einer Firewall-Richtlinie* (Seite 116).

Data Control

Data Control ist standardmäßig deaktiviert. Konfigurieren Sie zum Schutz vor ungewollten Datenverlusten Data Control-Richtlinien, um ungewollte Datenverluste zu verhindern. Anweisungen hierzu finden Sie unter *Data Control* (Seite 156).

Device Control

Device Control ist standardmäßig deaktiviert. Konfigurieren Sie zur Beschränkung zulässiger Hardware-Geräte Device Control-Richtlinien. Anweisungen hierzu finden Sie unter *Device Control* (Seite 171).

NAC

Network Access Control ist standardmäßig deaktiviert. Konfigurieren Sie NAC-Richtlinien, um den Computerzugriff bestimmten Bedingungen zu unterwerfen. Anweisungen hierzu finden Sie unter *Ändern einer NAC-Richtlinie* (Seite 152).

Patch

Die Patch-Analyse ist standardmäßig deaktiviert. Bei neuen Patch-Richtlinien ist die Analyse aktiviert. Nach Aktivierung der Patch-Analyse werden die Computer täglich auf fehlende Patches analysiert, sofern kein anderes Intervall ausgewählt wurde. Wenn Sie die Patch-Analyse

aktivieren bzw. deaktivieren oder das Analyseintervall ändern möchten, konfigurieren Sie anhand der Anweisungen im Abschnitt *Informationen zur Patch-Analyse* (Seite 190) Patch-Richtlinien.

Manipulationsschutz

Der Manipulationsschutz ist standardmäßig deaktiviert. Konfigurieren Sie zum Aktivieren des Manipulationsschutzes Manipulationsschutz-Richtlinien. Anweisungen hierzu finden Sie unter *Allgemeine Informationen* (Seite 187).

Web Control

Web Control ist standardmäßig deaktiviert. Anweisungen zum Aktivieren von Web Control und Konfigurieren entsprechender Richtlinien entnehmen Sie bitte dem Abschnitt *Informationen zur Web Control-Richtlinie* (Seite 192).

Festplattenverschlüsselung

Standardmäßig werden Festplatten auf Computern nicht verschlüsselt. Konfigurieren Sie Richtlinien zur Festplattenverschlüsselung (entsprechende Anweisungen entnehmen Sie bitte dem Abschnitt *Informationen zur Festplattenverschlüsselung* (Seite 179)), um Computerlaufwerke durch Verschlüsselung vor unbefugtem Zugriff zu schützen und weitere Einstellungen für Anmeldung und Recovery vorzunehmen.

4.3.5 Erstellen einer Richtlinie

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Richtlinieneinstellung** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So können Sie eine Richtlinie erstellen:

Hinweis: Sie können keine NAC-Richtlinien erstellen. NAC-Richtlinien können nur bearbeitet werden. Mehr dazu erfahren Sie unter *Ändern einer NAC-Richtlinie* (Seite 152).

1. Rechtsklicken Sie in der Ansicht **Endpoints** im Fensterbereich **Richtlinien** auf den Richtlinientyp, den Sie erstellen möchten (z.B. „Update-Richtlinie“), und wählen Sie **Richtlinie erstellen**.

   Es wird eine „Neue Richtlinie“ zur Liste hinzugefügt und ihr Name markiert.

2. Geben Sie der Richtlinie einen neuen Namen.
3. Doppelklicken Sie auf die neue Richtlinie. Geben Sie die gewünschten Einstellungen ein.

   Anweisungen zur Auswahl der Einstellungen finden Sie im Abschnitt zum Konfigurieren der entsprechenden Richtlinie.

Die erstellte Richtlinie kann nun auf Gruppen übertragen werden.

4.3.6 Übertragen einer Richtlinie auf eine Gruppe

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Markieren Sie im Fensterbereich **Richtlinien** die Richtlinie.
2. Klicken Sie auf die Richtlinie und ziehen Sie sie auf die Gruppe, auf die sie übertragen werden soll. Bestätigen Sie bei entsprechender Aufforderung, dass Sie den Vorgang fortsetzen möchten.

Hinweis: Sie können auch auf eine Gruppe rechtsklicken und die Option **Gruppenrichtliniendetails öffnen** wählen. Anschließend können Sie Richtlinien für die Gruppe aus den Dropdown-Menüs auswählen.

4.3.7 Ändern einer Richtlinie

Bei rollenbasierter Verwaltung:

- Hierzu müssen Sie zum Ändern der entsprechenden **Richtlinieneinstellung** berechtigt sein.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So ändern Sie eine Richtlinie für eine Gruppe oder Gruppen von Computern:

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf die Richtlinie, die Sie bearbeiten möchten.
2. Bearbeiten Sie die Einstellungen.

Anweisungen zum Konfigurieren unterschiedlicher Richtlinien finden Sie in den entsprechenden Abschnitten.

4.3.8 Umbenennen einer Richtlinie

Bei rollenbasierter Verwaltung:

- Hierzu müssen Sie zum Ändern der entsprechenden **Richtlinieneinstellung** berechtigt sein.
- Sie können keine Richtlinien umbenennen, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Hinweis: Sie können keine „Standard“-Richtlinie umbenennen.

So können Sie eine Richtlinie umbenennen:

1. Wählen Sie im Fensterbereich **Richtlinien** die Richtlinie, die Sie umbenennen möchten.

2. Rechtsklicken Sie darauf und wählen Sie **Richtlinie umbenennen**.

4.3.9 Löschen einer Richtlinie

Bei rollenbasierter Verwaltung:

- Hierzu müssen Sie zum Ändern der entsprechenden **Richtlinieneinstellung** berechtigt sein.
- Sie können keine Richtlinien löschen, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Hinweis: Sie können keine „Standard“-Richtlinie löschen.

So können Sie eine Richtlinie löschen:

1. Rechtsklicken Sie im Fensterbereich **Richtlinien** auf die Richtlinie, die Sie löschen möchten, und wählen Sie **Richtlinie löschen**.
2. Alle Gruppen, die die gelöschte Richtlinie verwenden, werden auf die Standardrichtlinie zurückgesetzt.

4.3.10 Anzeige der Gruppen einer Richtlinie

Verfahren Sie wie folgt, um festzustellen, auf welche Gruppen eine bestimmte Richtlinie übertragen wurde:

- Rechtsklicken Sie im Fensterbereich **Richtlinie** auf die Richtlinie und wählen Sie **Gruppen anzeigen, denen diese Richtlinie zugeordnet wurde.**

  Eine Liste der Gruppen wird angezeigt, die diese Richtlinie verwenden.

4.3.11 Prüfen, ob Computer die Gruppenrichtlinie verwenden

Sie können prüfen, ob alle Computer in einer Gruppe mit der entsprechenden Gruppenrichtlinie konform sind.

1. Markieren Sie die Gruppe, die Sie prüfen möchten.
2. Wechseln Sie in der Computerliste in die Ansicht **Endpoints** und betrachten Sie auf der Registerkarte **Status** die Spalte **Richtlinienkonformität**.
   - Wenn „Wie Richtlinie“ angezeigt wird, ist der Computer mit den Richtlinien der Gruppe konform.
   - Wenn ein gelbes Warnsymbol und der Text „Weicht von Richtlinie ab“ angezeigt werden, verwendet der Computer eine andere Richtlinie als die übrigen Computer in der Gruppe.

   Nähere Informationen zum Status der Sicherheitsfunktionen des Computers und der ihm zugewiesenen Richtlinien finden Sie im entsprechenden Abschnitt in der Ansicht **Endpoints** (z.B. Registerkarte **Antivirus-Details**).

Wenn Computer mit den Gruppenrichtlinien konform sein sollen, verfahren Sie anhand der Anweisungen im Abschnitt *Durchsetzen von Gruppenrichtlinien* (Seite 38).

4.3.12 Durchsetzen von Gruppenrichtlinien

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Korrektur – Updates und Scans** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wenn Computer gefunden werden, die nicht mit den Richtlinien Ihrer Gruppe konform sind, können Sie Gruppenrichtlinien für diese Computer übernehmen.

1. Markieren Sie die Computer, die von der Gruppenrichtlinie abweichen.
2. Rechtsklicken Sie auf die Auswahl und wählen Sie **Konformität mit**. Wählen Sie dann den passenden Richtlinientyp aus, z.B. **Antivirus- und HIPS-Gruppenrichtlinie**.

4.4 Ermitteln von Computern im Netzwerk

4.4.1 Auswahl der Methode zur Ermittlung von Computern

Computer, die mit Enterprise Console verwaltet werden sollen, müssen zunächst in Enterprise Console hinzugefügt werden. Sie können die Funktion „Computer ermitteln“ verwenden und eine von mehreren Optionen wählen, mit denen Sie Computer im Netzwerk suchen und zu Enterprise Console hinzufügen können. Folgende Optionen stehen zur Auswahl:

- *Importieren von Containern und Computern aus Active Directory* (Seite 38)
- *Ermitteln von Computern mit Active Directory* (Seite 39)
- *Ermitteln von Computern im Netzwerk* (Seite 40)
- *Ermitteln von Computern in einem IP-Bereich* (Seite 40)
- *Importieren von Computern aus einer Datei* (Seite 41)

Bei rollenbasierter Verwaltung ist die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich, um Computer zur Konsole hinzuzufügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

4.4.2 Importieren von Containern und Computern aus Active Directory

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Beim Importieren von Gruppen aus Active Directory wird die Active Directory-Containerstruktur abgerufen und in Enterprise Console als Computergruppenstruktur übernommen. Sie können entweder nur die Gruppenstruktur oder Gruppen und Computer importieren. Bei letzterer Option werden in Active Directory gefundene Computer in ihrer jeweiligen Gruppe statt in der Gruppe **Nicht zugewiesen** gespeichert.

Sie können sowohl „normale“ Gruppen haben, die Sie selbst erstellen und verwalten, als auch Gruppen, die von Active Directory importiert wurden. Sie können die importierten Gruppen auch mit Active Directory synchronisieren.

So werden Gruppen aus Active Directory importiert:

1. Klicken Sie in der Symbolleiste auf das Symbol **Computer ermitteln**.
2. Wählen Sie im Dialogfeld **Computer ermitteln** unter **Import aus Active Directory** die Option **Import** aus und klicken Sie auf **OK**.

   Sie können auch auf eine Gruppe rechtsklicken und Active Directory-Container über die Option **Import aus Active Directory** importieren.

   Der **Assistent zum Import aus Active Directory** wird gestartet.
3. Befolgen Sie die Anweisungen des Assistenten. Geben Sie bei entsprechender Aufforderung an, ob **Computer und Gruppen** oder **Nur Gruppen** importiert werden sollen.

Nach dem Import von Containern aus Active Directory können Sie Richtlinien auf die Gruppen übertragen. Mehr dazu erfahren Sie unter *Informationen zu Richtlinien* (Seite 31).

Nach dem Zuweisen der Richtlinien können Sie die Gruppen bei Bedarf mit Active Directory synchronisieren. Anweisungen hierzu finden Sie unter *Synchronisierung mit Active Directory* (Seite 44).

4.4.3 Ermitteln von Computern mit Active Directory

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Mit Active Directory können Sie Netzwerkcomputer ermitteln und in der Gruppe **Nicht zugewiesen** auflisten lassen.

1. Klicken Sie in der Symbolleiste auf das Symbol **Computer ermitteln**.
2. Wählen Sie im Dialogfeld **Computer ermitteln** die Option **Active Directory** und klicken Sie auf **OK**.
3. Nun müssen Sie einen Benutzernamen und ein Kennwort eingeben. Dies ist notwendig, wenn eine Anmeldung auf Ihren Computern erforderlich ist (z.B. Windows XP Service Pack 2).

   Bei dem Benutzerkonto muss es sich um ein Domänen-Administratorkonto oder ein Konto mit Vollzugriff auf die XP-Zielcomputer handeln.

   Wenn Sie ein Domäne-Konto verwenden, *müssen* Sie den Benutzernamen in der Form Domäne\Benutzer eingeben.
4. Wählen Sie im Dialogfeld **Computer ermitteln** die Domänen, die Sie durchsuchen möchten. Klicken Sie auf **OK**.
5. Klicken Sie auf die Gruppe **Nicht zugewiesen**, um die aufgefundenen Computer anzuzeigen.

Um die Computer zu verwalten, ziehen Sie sie in eine Gruppe.

4.4.4 Ermitteln von Computern im Netzwerk

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So können Sie eine Liste von Computern, die in Windows-Domänen und Arbeitsgruppen gefunden wurden, in die Gruppe **Nicht zugewiesen** aufnehmen:

1. Klicken Sie in der Symbolleiste auf das Symbol **Computer ermitteln**.
2. Wählen Sie im Dialogfeld **Computer ermitteln** die Option **Netzwerk** und klicken Sie auf **OK**.
3. Geben Sie in das Dialogfeld **Zugangsdaten** den Benutzernamen und das Kennwort eines Benutzerkontos mit den erforderlichen Rechten zum Abrufen der Computerinformationen ein.

   Bei dem Benutzerkonto muss es sich um ein Domänen-Administratorkonto oder ein Konto mit Vollzugriff auf die Zielcomputer handeln. Wenn Sie ein Domäne-Konto verwenden, *müssen* Sie den Benutzernamen in der Form Domäne\Benutzer eingeben.

   Sie können diesen Schritt überspringen, wenn auf den Zielcomputern keine Anmeldung erforderlich ist.
4. Wählen Sie im Dialogfeld **Computer ermitteln** die Domänen oder Arbeitsgruppen aus, die Sie suchen möchten. Klicken Sie auf **OK**.
5. Klicken Sie auf die Gruppe **Nicht zugewiesen**, um die aufgefundenen Computer anzuzeigen.

Um die Computer zu verwalten, ziehen Sie sie in eine Gruppe.

4.4.5 Ermitteln von Computern in einem IP-Bereich

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können Netzwerkcomputer über einen IP-Adressen-Bereich ermitteln und in der Gruppe **Nicht zugewiesen** auflisten lassen.

Hinweis: Sie können keine IPv6-Adressen verwenden.

1. Klicken Sie in der Symbolleiste auf das Symbol **Computer ermitteln**.
2. Wählen Sie im Dialogfeld **Computer ermitteln** die Option **IP-Bereich** und klicken Sie auf **OK**.
3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ins Dialogfeld **Zugangsdaten** ein. Dies ist notwendig, wenn eine Anmeldung auf Ihren Computern erforderlich ist (z.B. Windows XP Service Pack 2).

   Bei dem Benutzerkonto muss es sich um ein Domänen-Administratorkonto oder ein Konto mit Vollzugriff auf die XP-Zielcomputer handeln.

   Wenn Sie ein Domäne-Konto verwenden, *müssen* Sie den Benutzernamen in der Form Domäne\Benutzer eingeben.

   In das Feld **SNMP** können Sie den Namen der SNMP-Community eingeben.

4. Geben Sie im Dialogfeld **Computer ermitteln** den **Beginn des IP-Bereichs** und das **Ende des IP-Bereichs** ein. Klicken Sie auf **OK**.
5. Klicken Sie auf die Gruppe **Nicht zugewiesen**, um die aufgefundenen Computer anzuzeigen.

Um die Computer zu verwalten, ziehen Sie sie in eine Gruppe.

4.4.6 Importieren von Computern aus einer Datei

Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Damit Enterprise Console Ihre Computer auflistet, können Sie die Computernamen aus einer Datei importieren. Sie können eine Datei erstellen, die in etwa folgende Einträge beinhaltet:

```
[GroupName1]
 Domain1|Windows7|ComputerName1
 Domain1|Windows2008ServerR2|ComputerName2
```

Hinweis: Sie müssen die Gruppe, in die die Computer aufgenommen werden sollen, nicht angeben. Bei Eingabe von [] (ohne Leerzeichen zwischen den Klammern) als Gruppenname werden Computer in die Gruppe **Nicht zugewiesen** gestellt.

Hinweis: Die folgenden Betriebssystemsnamen sind möglich: Windows2000, Windows2000Server, WindowsXP, Windows2003, WindowsVista, Windows7, WindowsServer2008, Windows2008ServerR2, Windows8, WindowsServer2012, MACOSX, Linux und Unix.

Sowohl der Domänenname als auch das Betriebssystem sind optional. Ein solcher Eintrag kann folgendermaßen aussehen:

```
[GroupName1]
 ComputerName1
```

Computernamen werden folgendermaßen importiert:

1. Klicken Sie im Menü **Datei** auf **Computer aus Datei importieren**.
2. Markieren Sie die Datei im Browser-Fenster.
3. Klicken Sie auf die Gruppe **Nicht zugewiesen**, um die aufgefundenen Computer anzuzeigen.
4. Um die Computer zu verwalten, ziehen Sie sie in eine Gruppe.

4.5 Synchronisierung mit Active Directory

4.5.1 Informationen zur Synchronisierung mit Active Directory

In diesem Abschnitt wird die Synchronisierung mit Active Directory zusammengefasst.

Welche Vorteile bietet die Synchronisierung mit Active Directory?

Mithilfe der Synchronisierung mit Active Directory können Sie Enterprise Console-Gruppen mit Active Directory-Containern synchronisieren. Neue Computer und Container, die in Active Directory erkannt wurden, werden automatisch in Enterprise Console kopiert. Sie können außerdem erkannte Arbeitsplatzrechner mit Windows 2000 oder höher automatisch schützen. Damit wird die Zeit, in der Computer infiziert werden können, und der erforderliche Arbeitsaufwand zur Organisation und zum Schutz von Computern, reduziert.

Hinweis: Computer mit Windows Server-Betriebssystemen, Mac OS, Linux oder UNIX werden nicht automatisch geschützt. Sie müssen solche Computer manuell schützen.

Nach der Einrichtung der Synchronisierung können Sie die gewünschten Einstellungen für E-Mail-Benachrichtigungen vornehmen, mit denen ausgewählte Empfänger über bei zukünftigen Synchronisierungen entdeckte neue Computer und Container informiert werden. Wenn Sie Computer in synchronisierten Enterprise Console Gruppen automatisch schützen möchten, können Sie außerdem Benachrichtigungen bei Fehlfunktionen einrichten.

So funktioniert die Synchronisierung mit Active Directory

In Enterprise Console können Sie "normale", nicht synchronisierte Gruppen haben, die Sie selbst verwalten, und Gruppen, die mit Active Directory synchronisiert werden.

Wenn Sie die Synchronisierung einrichten, wählen oder erstellen Sie einen Synchronisierungspunkt, eine Enterprise Console-Gruppe, die mit einem Active Directory-Container synchronisiert wird. Alle Computer und Untergruppen im Active Directory-Container werden in Enterprise Console kopiert und mit Active Directory synchronisiert.

Hinweis: Nähere Informationen zu Synchronisierungspunkten finden Sie im Abschnitt *Was ist ein Synchronisierungspunkt?* (Seite 43). Nähere Informationen zu Synchronisierungspunkten finden Sie im Abschnitt *Was ist eine synchronisierte Gruppe?* (Seite 43).

Nachdem Sie die Synchronisierung mit Active Directory eingerichtet haben, stimmt der synchronisierte Teil der Enterprise Console-Gruppenstruktur mit dem Active Directory-Container überein, mit dem er synchronisiert wurde. Dies bedeutet Folgendes:

- Wenn ein neuer Computer zum Active Directory-Container hinzugefügt wird, erscheint er auch in der Enterprise Console.
- Wenn ein Computer aus Active Directory entfernt oder in einen nicht synchronisierten Container verschoben wird, wird der Computer in die Gruppe **Nicht zugewiesen** in Enterprise Console verschoben.

  Hinweis: Wenn ein Computer in die Gruppe **Nicht zugewiesen** verschoben wird, empfängt er keine neuen Richtlinien mehr.

- Wenn ein Computer von einem synchronisierten Container in einen anderen verschoben wird, wird der Computer von einer Enterprise Console-Gruppe in eine andere verschoben.
- Wenn ein Computer bei seiner ersten Synchronisierung bereits in einer Enterprise Console-Gruppe existiert, wird er von dieser Gruppe in die synchronisierte Gruppe verschoben, die mit seinem Speicherort in Active Directory übereinstimmt.
- Wenn ein Computer in eine neue Gruppe mit verschiedenen Richtlinien verschoben wird, werden die neuen Richtlinien an den Computer gesendet.

Standardmäßig erfolgt eine Synchronisierung alle 60 Minuten. Sie können das Synchronisierungsintervall bei Bedarf ändern.

So gehen Sie bei der Synchronisierung vor

Es ist Ihnen überlassen, welche Gruppen mit Active Directory synchronisiert und wie viele Synchronisierungspunkte eingerichtet werden. Sie müssen entscheiden, ob die Größe der Gruppen, die aufgrund der Synchronisierung erstellt werden, überschaubar ist. Sie sollten in der Lage sein, problemlos Software einzusetzen und Computer zu scannen und zu bereinigen. Dies ist besonders wichtig für den ersten Einsatz.

Wir empfehlen folgende Vorgehensweise:

1. Importieren Sie die Gruppenstruktur (ohne Computer) mithilfe der Funktion **Import aus Active Directory**. Anweisungen hierzu finden Sie unter *Importieren von Containern und Computern aus Active Directory* (Seite 38).
2. Prüfen Sie die importierte Gruppenstruktur und wählen Sie Ihre Synchronisierungspunkte.
3. Richten Sie Gruppenrichtlinien ein und übertragen Sie diese auf die Gruppen und Untergruppen. Anweisungen hierzu finden Sie unter *Erstellen einer Richtlinie* (Seite 35) und *Übertragen einer Richtlinie auf eine Gruppe* (Seite 36).
4. Synchronisieren Sie Ihre gewählten Synchronisierungspunkte nacheinander mithilfe von Active Directory. Anweisungen hierzu finden Sie unter *Synchronisierung mit Active Directory* (Seite 44).

4.5.2 Was ist ein Synchronisierungspunkt?

Ein *Synchronisierungspunkt* ist eine Enterprise Console-Gruppe, die auf einen Container (oder eine Unterstruktur) in Active Directory verweist. Ein Synchronisierungspunkt kann Synchronisierungsgruppen enthalten, die von Active Directory importiert wurden.

Im Fensterbereich **Gruppen** erscheint ein Synchronisierungspunkt folgendermaßen:

Sie *können* einen Synchronisierungspunkt verschieben, umbenennen oder löschen. Sie können außerdem Richtlinien und Synchronisierungseinstellungen ändern, u.a. die Einstellungen für den automatischen Schutz für einen Synchronisierungspunkt.

Sie können *keine* Untergruppen in einem Synchronisierungspunkt erstellen oder löschen oder andere Gruppen in den Synchronisierungspunkt verschieben. Sie können keine Computer in einen oder aus einem Synchronisierungspunkt verschieben.

4.5.3 Was ist eine synchronisierte Gruppe?

Eine *synchronisierte Gruppe* ist eine Untergruppe eines Synchronisierungspunkts, die von Active Directory importiert wurde.

Im Fensterbereich **Gruppen** erscheint eine synchronisierte Gruppe folgendermaßen:

Sie *können* Richtlinien ändern, die einer synchronisierten Gruppe zugewiesen wurden.

Außer Gruppenrichtlinien können Sie *keine* Einstellungen für synchronisierte Gruppen ändern. Sie können eine synchronisierte Gruppe weder umbenennen, verschieben noch löschen. Sie können Computer oder Gruppen nicht in die oder aus der Gruppe verschieben. Sie können in der Gruppe keine Untergruppen erstellen oder löschen. Sie können für die Gruppe keine Synchronisierungseinstellungen ändern.

4.5.4 Synchronisierung mit Active Directory

Vorbereitung und Voraussetzungen:

- Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).
- Auf Computern in synchronisierten Gruppen, die automatisch geschützt werden sollen, müssen zunächst die im Abschnitt *Vorbereiten der Installation der Virenschutzsoftware* (Seite 49) erläuterten Vorbereitungen getroffen werden.

Verfahren Sie zur Synchronisierung mit Active Directory wie folgt:

1. Rechtsklicken Sie auf eine Gruppe, die als Synchronisierungspunkt eingerichtet werden soll, und wählen Sie **Synchronisierung mit Active Directory**.

   Der **Assistent zur Synchronisierung mit Active Directory** wird gestartet.

2. Klicken Sie im Fenster **Überblick** des Assistenten auf **Weiter**.
3. Wählen oder erstellen Sie auf der Seite **Wählen Sie eine Enterprise Console-Gruppe** eine Enterprise Console-Gruppe, die stets mit Active Directory (Synchronisierungspunkt) synchronisiert werden soll. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Wählen Sie einen Active Directory-Container** einen Active Directory-Container, mit dem die Gruppe synchronisiert werden soll. Geben Sie den Namen des Containers ein (z.B. LDAP://CN=Computers,DC=domain_name,DC=local) oder klicken Sie auf **Durchsuchen**, um den Container in Active Directory aufzurufen. Klicken Sie auf **Weiter**.

   Wichtig: Wenn ein Computer in mehreren synchronisierten Active Directory-Containern vorhanden ist, führt dies zu dem Problem, dass Nachrichten endlos zwischen ihm und Enterprise Console gesendet werden. Jeder Computer sollte in Enterprise Console nur einmal aufgeführt werden.

5. Wenn Sie Computer mit Windows 2000 oder höher automatisch schützen möchten, wählen Sie auf der Seite **Automatischer Schutz von Computern** das Kontrollkästchen **Sophos Sicherheitssoftware automatisch installieren** und dann die zu installierende Software aus.

   Hinweis: Die Systemvoraussetzungen der Software entnehmen Sie bitte der Sophos Website (*http://www.sophos.de/products/all-sysreqs.html*).

   - Vor der Installation von **Compliance Control** (einem Sophos NAC Agent) auf Computern müssen Sie auf den Link zur Eingabe der URL des NAC-Servers klicken. Wenn Sophos NAC auf mehreren Servern installiert ist, geben Sie die URL des Computers ein, auf dem der Anwendungsserver ausgeführt wird, und nicht die des Computers mit der Datenbank.

- Konfigurieren Sie die **Firewall** vor der Bereitstellung im Netzwerk zur Zulassung der erwünschten Daten, Anwendungen und Prozesse. Die Firewall ist standardmäßig aktiviert und sperrt unnötigen Datenverkehr. Anweisungen entnehmen Sie bitte dem Abschnitt *Konfigurieren von Richtlinien > Konfigurieren der Firewall-Richtlinie*.
- Lassen Sie die Option **Erkennung von Fremdsoftware** ausgewählt, wenn die Software anderer Hersteller automatisch entfernt werden soll. Wenn das Update-Tool eines anderen Herstellers entfernt werden soll, lesen Sie bitte den Abschnitt *Entfernen von Fremdsoftware* (Seite 51).

Alle bei dieser und zukünftigen Synchronisierungen erkannten Computer mit Windows 2000 oder höher werden automatisch und in Übereinstimmung mit der jeweiligen Gruppenrichtlinie geschützt.

Wichtig: Computer mit Windows Server-Betriebssystemen, Mac OS, Linux oder UNIX können nicht automatisch geschützt werden. In diesem Fall muss der Schutz manuell eingerichtet werden. Lesen Sie dazu bitte die *Erweiterte Startup-Anleitung* zu Sophos Enterprise Console.

Hinweis: Der automatische Schutz kann jederzeit über das Dialogfeld **Synchronisierungseigenschaften** aktiviert oder deaktiviert werden. Anweisungen hierzu finden Sie unter *Ändern der Synchronisierungseigenschaften* (Seite 47).

Klicken Sie auf **Weiter**.

6. Wenn Sie Computer automatisch schützen wollen, geben Sie auf der Seite **Geben Sie Zugangsdaten für Active Directory ein** die Details eines Administratorkontos ein, das zur Installation von Software auf den Computern verwendet wird. Klicken Sie auf **Weiter**.
7. Geben Sie auf der Seite **Wählen Sie das Synchronisierungsintervall** an, wie oft die Enterprise Console-Gruppe mit dem Active Directory-Container synchronisiert werden soll. Die Vorgabe lautet 60 Minuten.

   Hinweis: Das Synchronisierungsintervall kann jederzeit über das Dialogfeld **Synchronisierungseigenschaften** geändert werden. Anweisungen hierzu finden Sie unter *Ändern der Synchronisierungseigenschaften* (Seite 47).

8. Prüfen Sie die Angaben auf der Seite **Bestätigen Sie Ihre Auswahl** und klicken Sie dann auf **Weiter**, um fortzufahren.
9. Auf der letzten Seite des Assistenten können Sie die Details der Gruppen und Computer ansehen, die synchronisiert wurden.

   Sie können außerdem E-Mail-Benachrichtigungen über neue Computer und Gruppen, die bei zukünftigen Synchronisierungen gefunden werden, an die von Ihnen gewählten Empfänger senden lassen. Wenn Sie Computer in synchronisierten Gruppen automatisch schützen möchten, können Sie außerdem Benachrichtigungen für das Fehlschlagen des automatischen Schutzes einrichten. Klicken Sie auf **Beenden** und aktivieren Sie das Kontrollkästchen auf der letzten Seite des Assistenten. Das Dialogfeld **E-Mail-Benachrichtigungen konfigurieren** wird geöffnet. Anweisungen hierzu finden Sie unter *Einrichten von E-Mail-Benachrichtigungen für Active Directory-Synchronisierung* (Seite 209).

   Klicken Sie zum Schließen des Assistenten auf **Fertig stellen**.

4.5.5 Automatisches Schützen von Computern über Synchronisierung

Vorbereitung und Voraussetzungen:

- Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).
- Sie müssen die Computer anhand der Anweisungen im Abschnitt *Vorbereiten der Installation der Virenschutzsoftware* (Seite 49) auf die automatische Installation von Sicherheitssoftware vorbereitet haben.

Arbeitsplatzrechner mit Windows 2000 oder höher können automatisch geschützt werden, wenn sie während der Synchronisierung mit Active Directory erkannt werden.

Wichtig: Computer mit Windows Server-Betriebssystemen, Mac OS, Linux oder UNIX können nicht automatisch geschützt werden. In diesem Fall muss der Schutz manuell eingerichtet werden. Lesen Sie dazu bitte die *Erweiterte Startup-Anleitung* zu Sophos Enterprise Console.

Der automatische Schutz von Computern in synchronisierten Gruppen lässt sich beim Einrichten der Synchronisierung (siehe *Synchronisierung mit Active Directory* (Seite 44)) oder durch das nachträgliche Ändern der Synchronisierungseigenschaften aktivieren.

Im Folgenden wird die Aktivierung des Schutzes von Computern in den Synchronisierungseigenschaften beschrieben.

1. Wählen Sie im Bereich **Gruppen** die Gruppe (Synchronisierungspunkt), für die Sie den automatischen Schutz aktivieren möchten. Rechtsklicken Sie auf die Gruppe und wählen Sie **Synchronisierungseigenschaften**.
2. Wählen Sie im Dialogfenster **Eigenschaften der Synchronisierung** das Kontrollkästchen **Sophos Sicherheitssoftware automatisch installieren** und dann die zu installierende Software aus.
   - Vor der Installation von **Compliance Control** (einem Sophos NAC Agent) auf Computern müssen Sie auf den Link zur Eingabe der URL des NAC-Servers klicken. Wenn Sophos NAC auf mehreren Servern installiert ist, geben Sie die URL des Computers ein, auf dem der Anwendungsserver ausgeführt wird, und nicht die des Computers mit der Datenbank.
   - Konfigurieren Sie die **Firewall** vor der Bereitstellung im Netzwerk zur Zulassung der erwünschten Daten, Anwendungen und Prozesse. Die Firewall ist standardmäßig aktiviert und sperrt unnötigen Datenverkehr. Anweisungen entnehmen Sie bitte dem Abschnitt *Konfigurieren von Richtlinien > Konfigurieren der Firewall-Richtlinie*.
   - Lassen Sie die Option **Erkennung von Fremdsoftware** ausgewählt, wenn die Software anderer Hersteller automatisch entfernt werden soll. Wenn das Update-Tool eines anderen Herstellers entfernt werden soll, lesen Sie bitte den Abschnitt *Entfernen von Fremdsoftware* (Seite 51).
3. Geben Sie die Zugangsdaten eines zur Softwareinstallation befugten Administratorkontos ein. Klicken Sie auf **OK**.

Sie können den automatischen Schutz später deaktivieren, indem Sie im Dialogfeld **Synchronisierungseigenschaften** das Kontrollkästchen neben **Sophos Sicherheitssoftware automatisch installieren** deaktivieren.

4.5.6 Ändern der Synchronisierungseigenschaften

Vorbereitung und Voraussetzungen:

- Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).
- Auf Computern in synchronisierten Gruppen, die automatisch geschützt werden sollen, müssen zunächst die im Abschnitt *Vorbereiten der Installation der Virenschutzsoftware* (Seite 49) erläuterten Vorbereitungen getroffen werden.

So ändern Sie die Synchronisierungseigenschaften:

1. Wählen Sie im Fensterbereich **Gruppen** die Gruppe (Synchronisierungspunkt), für die Sie Synchronisierungseigenschaften bearbeiten möchten. Rechtsklicken Sie auf die Gruppe und wählen Sie **Synchronisierungseigenschaften**.

   Das Dialogfeld **Synchronisierungseigenschaften** wird angezeigt.

2. Im Feld **Active Directory-Container** wird der Container angezeigt, mit dem die Gruppen synchronisiert wurde. Wenn Sie die Gruppe mit einem anderen Active Directory-Container synchronisieren möchten, entfernen Sie die Synchronisierung und starten Sie nochmals den **Assistenten zur Synchronisierung mit Active Directory**. Nähere Informationen finden Sie unter *Aktivieren/Deaktivieren der Synchronisierung* (Seite 48) und *Synchronisierung mit Active Directory* (Seite 44).
3. Legen Sie im Feld **Synchronisierungsintervall** die Häufigkeit der Synchronisierung fest. Die Vorgabe lautet 60 Minuten. Der Mindestwert beträgt 5 Minuten.
4. Aktivieren Sie das Kontrollkästchen **Sophos Sicherheitssoftware automatisch installieren**, wenn Sie alle neu erkannten Windows 2000- oder neueren Arbeitsplatzrechner in Übereinstimmung mit der jeweiligen Gruppenrichtlinie automatisch schützen möchten. Virenschutz ist im Bereich **Funktionen** standardmäßig aktiviert. Wenn noch andere Sophos Sicherheitssoftware installiert werden soll, aktivieren Sie die entsprechenden Kontrollkästchen. Geben Sie die Zugangsdaten eines zur Softwareinstallation befugten Administratorkontos ein.

   Hinweis: Bevor Sie Sophos NAC auf Computern installieren können, müssen Sie auf den Link zur Eingabe der URL des NAC-Servers klicken.

Hinweis: Nur Arbeitsplatzrechner mit Windows 2000 oder höher können automatisch geschützt werden. Computer mit Windows Server-Betriebssystemen, Mac OS, Linux oder UNIX können nicht automatisch geschützt werden. In diesem Fall muss der Schutz manuell eingerichtet werden. Lesen Sie dazu bitte die *Erweiterte Startup-Anleitung* zu Sophos Enterprise Console.

4.5.7 Sofortige Synchronisierung mit Active Directory

Vorbereitung und Voraussetzungen:

- Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).
- Auf Computern in synchronisierten Gruppen, die automatisch geschützt werden sollen, müssen zunächst die im Abschnitt *Vorbereiten der Installation der Virenschutzsoftware* (Seite 49) erläuterten Vorbereitungen getroffen werden.

Wenn Sie nicht auf das nächste Synchronisierungsintervall warten möchten, lassen sich Enterprise Console-Gruppen (Synchronisierungspunkte) auch sofort mit Active Directory-Containern synchronisieren.

So wird eine sofortige Synchronisierung durchgeführt:

1. Wählen Sie im Fensterbereich **Gruppen** die Gruppe (Synchronisierungspunkt), die mit Active Directory synchronisiert werden soll. Rechtsklicken Sie auf die Gruppe und wählen Sie **Synchronisierungseigenschaften**.
2. Wenn Sie die gewünschten Änderungen vorgenommen haben, klicken Sie auf **OK**.

4.5.8 Aktivieren/Deaktivieren der Synchronisierung

Vorbereitung und Voraussetzungen:

- Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).
- Auf Computern in synchronisierten Gruppen, die automatisch geschützt werden sollen, müssen zunächst die im Abschnitt *Vorbereiten der Installation der Virenschutzsoftware* (Seite 49) erläuterten Vorbereitungen getroffen werden.

Verfahren Sie zum Aktivieren/Deaktivieren der Synchronisierung mit Active Directory wie folgt:

- Zum Aktivieren der Synchronisierung starten Sie den **Assistent zur Synchronisierung mit Active Directory** (siehe Abschnitt *Synchronisierung mit Active Directory* (Seite 44)).
- Um die Synchronisierung zu deaktivieren, rechtsklicken Sie auf die Gruppe (Synchronisierungspunkt), die Sie nicht mehr mit Active Directory synchronisieren möchten, und wählen Sie **Synchronisierung entfernen**. Klicken Sie zur Bestätigung auf **Ja**.

5 Schützen von Computern

5.1 Allgemeine Informationen

Sie können Sophos Sicherheitssoftware wie folgt installieren:

- Zum automatischen Schutz von Computern können Sie den Assistenten zum Schützen von Computern in Enterprise Console verwenden (siehe *Automatisches Schützen von Computern* (Seite 51)).
- Ferner können Sie Computer mittels Synchronisierung von Active Directory manuell schützen (siehe *Informationen zur Synchronisierung mit Active Directory* (Seite 41)).
- Zum manuellen Schutz von Computern können Sie die erforderliche Software mit Enterprise Console auffinden (siehe *Auffinden der Installationsprogramme für den manuellen Schutz von Computern* (Seite 55)). Gehen Sie dann zum gewünschten Computer und installieren Sie die Sicherheitssoftware manuell.

5.2 Vorbereiten der Installation der Virenschutzsoftware

Sie müssen nicht nur dafür sorgen, dass die allgemeinen Systemanforderungen erfüllt werden, es sind außerdem noch weitere Schritte notwendig, bevor auf den Computern Software automatisch installiert werden kann.

Hinweis: Die automatische Installation ist unter Mac, Linux und UNIX nicht möglich.

In Active Directory können Sie Computer mit einem Gruppenrichtlinienobjekt (GPO) vorbereiten. Anweisungen entnehmen Sie bitte dem Sophos Support-Artikel 116754 (*http://www.sophos.de/support/knowledgebase/article/116754.html*).

Wenn Sie Arbeitsgruppen verwenden, müssen Sie die Computer lokal konfigurieren. Anweisungen entnehmen Sie bitte dem Sophos Support-Artikel 116755 (*http://www.sophos.de/support/knowledgebase/article/116755.html*).

5.3 Vorbereiten der Installation von Verschlüsselungssoftware

Sie müssen nicht nur dafür sorgen, dass die allgemeinen Systemanforderungen erfüllt werden, es sind außerdem noch weitere Schritte notwendig, bevor auf den Computern Software automatisch installiert werden kann.

So bereiten Sie die Computer auf die Installation von Verschlüsselungssoftware vor:

1. Stellen Sie sicher, dass mit Fremdsoftware verschlüsselte Laufwerke entschlüsselt wurden und die Fremdsoftware deinstalliert wurde.
2. Erstellen Sie ein komplettes Backup der Daten.
3. Überprüfen Sie, ob ein Windows-Benutzerkonto mit Zugangsdaten für den Benutzer auf dem Endpoint eingerichtet und aktiv ist.
4. Stellen Sie vor der Bereitstellung der Festplattenverschlüsselung sicher, dass die Computer bereits mit Virenschutzsoftware von Sophos (Version 10) geschützt werden.

5. Deinstallieren Sie Boot-Manager anderer Anbieter, z.B. PROnetworks Boot Pro und Boot-US.
6. Überprüfen Sie die Festplatte(n) über folgenden Befehl auf Fehler: „**chkdsk %drive% /F /V /X**“. Unter Umständen werden Sie dazu aufgefordert, den Computer neu zu starten und **chkdsk** noch einmal auszuführen.

   Nähere Informationen finden Sie unter *http://www.sophos.de/support/knowledgebase/article/107081.html*.

   Die Ergebnisse (Log-Datei) können Sie in der Windows-Ereignisanzeige prüfen.

   - Windows XP: Wählen **Anwendung**, **Windows-Anmeldung**.
   - Windows 7, Windows Vista: Wählen Sie **Windows-Protokolle**, **Anwendung**, **Wininit**.

7. Benutzen Sie das Windows-Tool **defrag**, um fragmentierte Boot-Dateien, Datendateien und Ordner auf lokalen Laufwerken aufzufinden und zu konsolidieren: „**defrag %Laufwerk%** “.

   Nähere Informationen finden Sie unter *http://www.sophos.de/support/knowledgebase/article/109226.html*.

8. Wenn Sie ein Image/Clone-Programm verwendet haben, muss der MBR unter Umständen bereinigt werden. Starten Sie den Computer von einer Windows-DVD und führen Sie den Befehl **FIXMBR** innerhalb der Windows Recovery Console aus. Nähere Informationen finden Sie unter *http://www.sophos.de/support/knowledgebase/article/108088.html*.
9. Wenn die Bootpartition auf dem Computer von FAT nach NTFS konvertiert wurde, der Computer aber noch nicht neu gestartet wurde, sollten Sie den Computer neu starten. Andernfalls wird die Installation unter Umständen nicht abgeschlossen.
10. Öffnen Sie die Windows-Firewall mit erweiterter Sicherheit. Öffnen Sie in der Systemsteuerung die **Verwaltung**. Stellen Sie sicher, dass **Eingehende Verbindungen** zugelassen werden. Lassen Sie unter **Eingehende Regeln** die folgenden Prozesse zu.

    Remoteverwaltung (NP eingehend) Domäne

    Remoteverwaltung (NP eingehend) Privat

    Remoteverwaltung (RPC) Domäne

    Remoteverwaltung (RPC) Privat

    Remoteverwaltung (RPC-EPMAP) Domäne

    Remoteverwaltung (RPC-EPMAP) Privat

    Verfahren Sie nach Abschluss der Installation wie folgt:

    - Wenn Sie weitere Funktionen auf den Endpoints installieren und die Windows-Firewall weiterhin nutzen möchten, können Sie den Prozess bei Bedarf wieder deaktivieren.
    - Wenn Sie weitere Funktionen auf den Endpoints installieren möchten, deaktivieren Sie die Dienste erst nach der Installation sämtlicher Funktionen.

5.4 Entfernen von Fremdsoftware

Wenn Sie installierte Sicherheitssoftware entfernen möchten, sollten Sie zunächst wie folgt verfahren, bevor Sie **Erkennung von Fremdsoftware** im Assistenten zum **Schutz von Computern** auswählen und installieren:

- Sollte auf einigen Computern die Virenschutzsoftware anderer Hersteller laufen, schließen Sie die Benutzeroberfläche.
- Sollte auf einigen Computern die Firewall oder das HIPS-Produkt eines anderen Herstellers laufen, deaktivieren Sie diese Software oder stellen Sie sie so ein, dass das Sophos Installationsprogramm ausgeführt werden kann.
- Wenn nicht nur die Software sondern auch das Update-Tool eines anderen Herstellers entfernt werden soll (damit eine automatische Neuinstallation verhindert wird), führen Sie bitte die folgenden Schritte aus. Falls auf den Computern kein Update-Tool installiert wurde, ignorieren Sie diese Schritte.

Hinweis: Computer, auf denen die Software anderer Hersteller entfernt wurde, müssen anschließend neu gestartet werden.

Wenn auf Computern ein Update-Tool eines anderen Herstellers installiert ist und es entfernt werden soll, muss die Konfigurationsdatei geändert werden, bevor im **Assistenten zum Schutz von Computern** die **Erkennung von Fremdsoftware** ausgeführt werden kann:

Hinweis: Wenn auf Computern ein Firewall- oder HIPS-Produkt eines anderen Herstellers installiert ist, lassen Sie das entsprechende Update-Tool unberührt. Für weitere Informationen lesen Sie die Dokumentation des anderen Herstellers.

So ändern Sie die Konfigurationsdatei:

1. Suchen Sie im zentralen Installationsverzeichnis die Datei „data.zip“.
2. Extrahieren Sie die Konfigurationsdatei „crt.cfg“ aus der Datei „data.zip“.
3. Ändern Sie in der Datei „crt.cfg“ die Zeile „RemoveUpdateTools=0“ in „RemoveUpdateTools=1“.
4. Speichern Sie Ihre Änderungen und speichern Sie „crt.cfg“ im gleichen Verzeichnis wie „data.zip“. Legen Sie „crt.cfg“ nicht wieder in „data.zip“ ab, weil die Datei sonst beim nächsten Update überschrieben wird.

Wenn Sie den Assistenten zum **Schutz von Computern** ausführen und die **Erkennung von Fremdsoftware** auswählen, entfernt die geänderte Konfigurationsdatei jegliche Sicherheits-Tools und Sicherheitssoftware von anderen Anbietern.

5.5 Automatisches Schützen von Computern

Treffen Sie zunächst folgende Vorbereitungen:

- Sie müssen der Gruppe eine Update-Richtlinie zuweisen. Erst dann können die Computer in der Gruppe geschützt werden.

- Sie müssen die Computer anhand der Anweisungen im Abschnitt *Vorbereiten der Installation der Virenschutzsoftware* (Seite 49) auf die automatische Installation von Sicherheitssoftware vorbereitet haben.
- Bei rollenbasierter Verwaltung ist hierzu die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Die automatische Installation ist unter Mac, Linux und UNIX nicht möglich. Führen Sie die Installation auf diesen Betriebssystemen manuell durch. Nähere Anweisungen entnehmen Sie bitte der *Erweiterten Startup-Anleitung* zu Sophos Enterprise Console. Begleitmaterial zu Sophos Software finden Sie hier: *www.sophos.de/support/docs/*.

Wenn Sie mit Active Directory synchronisieren und die Computer automatisch schützen, müssen Sie die nachfolgenden Schritte *nicht* befolgen. Details entnehmen Sie bitte dem Abschnitt *Informationen zur Synchronisierung mit Active Directory* (Seite 41) und vergleichbaren Kapiteln.

Zum automatischen Schutz von Computern sind folgende Schritte erforderlich:

1. Verfahren Sie in Abhängigkeit davon, ob sich die Computer bereits in der Gruppe befinden, anhand einer der folgenden Methoden:
   - Wenn sich die Computer, die Sie schützen möchten, in der Gruppe **Nicht zugewiesen** befinden, ziehen Sie sie in eine Gruppe.
   - Wenn die Computer bereits einer Gruppe zugewiesen wurden, wählen Sie sie aus, rechtsklicken Sie darauf und klicken Sie auf **Computer schützen**.

   Der **Assistent zum Schutz von Computern** wird gestartet.

2. Befolgen Sie die Anweisungen des Assistenten. Wählen Sie auf der Seite **Funktionsauswahl** die gewünschten Funktionen aus.

   Hinweis: Die Systemvoraussetzungen der Funktionen entnehmen Sie bitte der Sophos Website (*http://www.sophos.de/products/all-sysreqs.html*).

   Diverse Funktionen, wie etwa der Virenschutz, sind immer ausgewählt und müssen installiert werden. Sie können auch folgende Funktionen installieren: Manche Funktionen stehen nur bei entsprechender Lizenzierung zur Verfügung.

   - **Firewall**

     Konfigurieren Sie die Firewall vor der Bereitstellung im Netzwerk zur Zulassung der erwünschten Daten, Anwendungen und Prozesse. Die Firewall ist standardmäßig aktiviert und sperrt unnötigen Datenverkehr. Anweisungen entnehmen Sie bitte dem Abschnitt *Konfigurieren von Richtlinien > Konfigurieren der Firewall-Richtlinie*.
   - **Compliance Control** (ein Agent für Sophos NAC)

     Vor dem Einsatz von Compliance Control müssen Sie die NAC-Server-URL angeben. Wenn Sophos NAC auf mehreren Servern installiert ist, geben Sie die URL des Computers ein, auf dem der Anwendungsserver ausgeführt wird, und nicht die des Computers mit der Datenbank.
   - **Patch**

- **Erkennung von Fremdsoftware**

  Lassen Sie die Option **Erkennung von Fremdsoftware** ausgewählt, wenn die Software anderer Hersteller automatisch entfernt werden soll. Durch die Erkennung von Fremdsoftware werden nur Produkte mit demselben Funktionsumfang wie die von Ihnen installierten Produkte deinstalliert. Wenn das Update-Tool eines anderen Herstellers entfernt werden soll, lesen Sie bitte den Abschnitt *Entfernen von Fremdsoftware* (Seite 51).

3. Auf der Seite **Schutz-Übersicht** werden Installationsprobleme in der Spalte **Sicherheitshinweise** angezeigt. Beheben Sie die Installationsprobleme anhand der Anweisungen im Abschnitt *Sophos Endpoint Security and Control konnte nicht installiert werden* (Seite 242) oder führen Sie auf diesen Computern die Installation manuell durch (mehr Informationen hierzu können Sie der *Erweiterten Startup-Anleitung* zu *Sophos Enterprise Console* entnehmen). Klicken Sie auf **Weiter**.
4. Geben Sie auf der Seite **Zugangsdaten** die Zugangsdaten eines Kontos ein, mit dem Software installiert werden kann.

   Bei diesem Konto handelt es sich in der Regel um ein Domänen-Administratorkonto. Das Konto muss:

   - lokale Administratorrechte auf den Computern haben, die Sie schützen möchten.
   - sich auf dem Computer anmelden können, auf dem Sie den Management-Server installiert haben.
   - Lesezugriff auf den Primary Server-Ort haben, der in der **Update**-Richtlinie angegeben wurde. Nähere Informationen finden Sie unter *Update-Server-Standorte* (Seite 84) und anderen Abschnitten zum *Konfigurieren der Update-Server-Standorte*.

   Hinweis: Wenn Sie ein Domäne-Konto verwenden, *müssen* Sie den Benutzernamen in der Form **Domäne\Benutzer** eingeben.

   Wenn Computer auf unterschiedlichen Domänen demselben Active Directory-Schema unterliegen, verwenden Sie das Unternehmensadministratorkonto von Active Directory.

5.6 Automatische Installation von Verschlüsselungssoftware

Warnhinweis: Bei der Erstinstallation von Sophos Verschlüsselungssoftware empfiehlt sich, alle Einstellungen schrittweise zu aktivieren und zu testen.

Sie können die Verschlüsselungssoftware automatisch unter Windows XP, Windows Vista und Windows 7 installieren.

Verfahren Sie vor der Installation der Software auf Computern wie folgt:

- Stellen Sie sicher, dass mit Fremdsoftware verschlüsselte Laufwerke entschlüsselt wurden und die Fremdsoftware deinstalliert wurde.
- Erstellen Sie ein komplettes Backup der Daten.

Führen Sie zudem folgende Vorbereitungen durch:

- Stellen Sie sicher, dass Sie die Schritte im Abschnitt *Vorbereiten der Installation von Verschlüsselungssoftware* (Seite 49) abgearbeitet haben (insbesondere die Installation von Sophos Antiviren-Software, Version 10).
- Stellen Sie sicher, dass Sie Verschlüsselungssoftware abonniert und heruntergeladen haben. Nähere Informationen finden Sie unter *Abonnieren von Verschlüsselungssoftware* (Seite 81).
- Bei rollenbasierter Verwaltung müssen Sie zur Installation und Konfiguration von Verschlüsselung auf Computern über die Berechtigungen **Computersuche, -schutz und -gruppe** und **Richtlinieneinstellung – Festplattenverschlüsselung** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Verfahren Sie zur automatischen Installation von Verschlüsselungssoftware wie folgt:

1. Wählen Sie in Enterprise Console alle Computer aus, auf denen die Festplattenverschlüsselung installiert werden soll.
2. Rechtsklicken Sie auf Computer und klicken Sie anschließend auf **Computer schützen**. Der **Assistent zum Schutz von Computern** wird gestartet.
3. Klicken Sie im Eröffnungsfenster auf **Weiter**.
4. Wählen Sie auf der Seite **Installationsart Verschlüsselungssoftware** aus.
5. Wenn mehrere Verschlüsselungsabonnements und Installer-Verzeichnisse (Bootstrap-Verzeichnisse) vorhanden sind, wird die Seite **Verschlüsselungsverzeichnis** angezeigt. Wählen Sie das **Verschlüsselungsabonnement** und geben Sie die **Adresse** an, von der installiert werden soll.
6. Auf der Seite **Verschlüsselungsübersicht** werden Installationsprobleme in der Spalte **Sicherheitshinweise** angezeigt. Beheben Sie die Installationsprobleme anhand der Anweisungen im Abschnitt *Sophos Endpoint Security and Control konnte nicht installiert werden* (Seite 242) oder führen Sie auf diesen Computern die Installation manuell durch (mehr Informationen hierzu können Sie der *Erweiterten Startup-Anleitung für Sophos Enterprise Console* entnehmen).
7. Geben Sie auf der Seite **Zugangsdaten** die Zugangsdaten eines Kontos ein, mit dem Software installiert werden kann.

   Bei diesem Konto handelt es sich in der Regel um ein Domänen-Administratorkonto. Das Konto muss:

   - lokale Administratorrechte auf den Computern haben, die Sie schützen möchten.
   - sich auf dem Computer anmelden können, auf dem Sie den Management Server installiert haben.
   - Lesezugriff auf den Primary Server-Ort haben, der in der **Update**-Richtlinie angegeben wurde. Nähere Informationen finden Sie unter *Update-Server-Standorte* (Seite 84) und anderen Abschnitten zum *Konfigurieren der Update-Server-Standorte*.

   Hinweis: Wenn Sie ein Domäne-Konto verwenden, *müssen* Sie den Benutzernamen in der Form **Domäne\Benutzer** eingeben.

   Wenn Computer auf unterschiedlichen Domänen demselben Active Directory-Schema unterliegen, verwenden Sie das Unternehmensadministratorkonto von Active Directory.

Die Installation erfolgt gestaffelt. Es kann also einige Minuten dauern, bis der Vorgang auf allen Computern abgeschlossen ist.

Etwa 30 Minuten nach der Installation der Verschlüsselungssoftware werden Computer automatisch neu gestartet.

Die Festplattenverschlüsselung ist standardmäßig nicht nach der Installation aktiviert. Wenn Sie sie aktivieren möchten, konfigurieren Sie die Richtlinie zur Festplattenverschlüsselung nach Ihren Wünschen und übertragen Sie sie auf die Computer. Nähere Informationen finden Sie unter *Konfigurieren der Festplattenverschlüsselung* (Seite 180).

Nähere Informationen zum Startverhalten des Computers und der ersten Anmeldung nach der Installation und Aktivierung der Festplattenverschlüsselung entnehmen Sie bitte der *Sophos Disk Encryption 5.61 Benutzerhilfe* oder der *Enterprise Console Schnellstartanleitung/Erweiterten Startup-Anleitung*.

5.7 Auffinden der Installationsprogramme für den manuellen Schutz von Computern

Wenn Enterprise Console auf bestimmten Computern die Virenschutz-, Firewall-, NAC- oder Patch-Funktion nicht automatisch installieren kann, können Sie die Installation manuell durchführen.

So können Sie die Installationsprogramme auffinden:

1. Klicken Sie im Menü **Ansicht** auf **Bootstrap-Verzeichnisse**.
2. Im Dialogfeld **Bootstrap-Verzeichnisse** werden für die einzelnen Software-Abonnements die Verzeichnisse mit den Installern sowie die unterstützten Plattformen und Software-Versionen angezeigt. Schreiben Sie sich den Speicherort der benötigten Datei auf.

   Wenn die Festplattenverschlüsselung in Ihrer Lizenz inbegriffen ist, müssen die Endpoints auf die Verschlüsselung vorbereitet werden. Installieren Sie zunächst die Virenschutzsoftware von Sophos in der Version 10. Installieren Sie im Anschluss die Verschlüsselungssoftware. Der Standort des Installationsprogramms mit Verschlüsselung (setup.exe) wird angezeigt.

Anweisungen zur manuellen Installation von Sicherheitssoftware auf unterschiedlichen Betriebssystemen finden Sie in der *Erweiterten Startup-Anleitung* zu *Sophos Enterprise Console* .

Etwa 30 Minuten nach der Installation der Verschlüsselungssoftware werden Computer automatisch neu gestartet.

Nähere Informationen zum Startverhalten des Computers und der ersten Anmeldung nach der Installation und Aktivierung der Festplattenverschlüsselung entnehmen Sie bitte der *Sophos Disk Encryption Benutzerhilfe* oder der *Enterprise Console Schnellstartanleitung/Erweiterten Startup-Anleitung*.

5.8 Ermitteln des Netzwerkschutzes

5.8.1 So überprüfen Sie, ob Ihr Netzwerk geschützt ist

Das Dashboard bietet Ihnen einen Überblick über den Sicherheitsstatus des Netzwerks. Mehr dazu erfahren Sie unter *Dashboard-Bereiche* (Seite 7) und *Konfigurieren des Dashboards* (Seite 56).

Mit Computerlisten und Computerlistenfiltern können Sie problematische Computer ermitteln. So können Sie beispielsweise Computer auffinden, auf denen keine Firewall oder Patch-Analyse installiert ist, oder auf denen Meldungen angezeigt werden, bei denen Benutzereingriff erforderlich ist. Mehr dazu erfahren Sie unter *Überprüfen, ob die Computer geschützt sind* (Seite 57), *Überprüfen, ob sich die Computer auf dem neuesten Stand befinden* (Seite 57) und *Auffinden von Computern mit Problemen* (Seite 58).

Zudem können Sie überprüfen, ob alle Computer in einer Gruppe mit den Richtlinien der Gruppe übereinstimmen. Details hierzu finden Sie im Abschnitt *Prüfen, ob Computer die Gruppenrichtlinie verwenden* (Seite 37).

5.8.2 Konfigurieren des Dashboards

Bei rollenbasierter Verwaltung müssen Sie zur Konfiguration des Dashboards über die Berechtigung **Systemkonfiguration** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Im Dashboard wird auf der Basis des Prozentsatzes der verwalteten Computer, auf denen Alerts oder Fehler ausstehen, oder der Zeit, die seit dem letzten Update von Sophos vergangen ist, angezeigt, wenn eine Warnstufe oder kritische Stufe erreicht wurde.

Sie können die Warnstufen bzw. kritischen Stufen nach Ihren Wünschen konfigurieren.

1. Klicken Sie im Menü **Extras** auf die Option **Dashboard konfigurieren**.
2. Ändern Sie im Dialogfeld **Dashboard konfigurieren** die zulässigen Höchstwerte in den Textfeldern **Warnstufe** und **Kritische Stufe**. Anweisungen hierzu finden Sie im Folgenden.

   a) Geben Sie in die Felder **Computer mit ausstehenden Alerts**, **Computer mit fehlerhaften Sophos Produkten** und **Richtlinien und Schutz** den Prozentsatz aller Computer an, die von einem bestimmten Problem maximal betroffen sein dürfen, bis sich die Anzeige in „Warnung“ oder „kritisch“ ändert.

   b) Geben Sie in das Feld **Computer mit Ereignissen** die Anzahl an Ereignissen ein, die binnen 7 Tagen stattfinden dürfen sollen, bis ein Alert im Dashboard angezeigt wird.

   c) Geben Sie unter **Letztes Update von Sophos** die Zeit in Stunden, die seit dem letzten erfolgreichen Update von Sophos verstreichen darf, bis die Update-Anzeige von „Warnung“ auf „Kritisch“ geändert wird. Klicken Sie auf **OK**.

   Wenn Sie eine Stufe auf Null setzen, wird bei Empfang des ersten Alerts ein Warnhinweis ausgegeben.

Sie können außerdem E-Mail-Benachrichtigungen einstellen, die an die gewählten Empfänger gesendet werden sollen, wenn ein Warn- oder ein kritischer Schwellenwert überschritten wurde. Genaue Anweisungen finden Sie unter *Einrichten von Netzwerkstatus-E-Mail-Benachrichtigungen* (Seite 209).

5.8.3 Überprüfen, ob die Computer geschützt sind

Computer sind geschützt, wenn On-Access-Scans und Firewall (sofern installiert) aktiv sind. Für einen vollständigen Schutz muss sich die Software außerdem auf dem neuesten Stand befinden.

Hinweis: Möglicherweise haben Sie sich entschieden, bei bestimmten Computertypen, z.B. auf Fileservern, die On-Access-Scanfunktion zu deaktivieren. Stellen Sie in diesem Fall sicher, dass auf diesen Computern geplante Scans laufen und dass sie aktuell sind.

So überprüfen Sie, ob die Computer geschützt sind:

1. Markieren Sie die Computergruppe, die Sie prüfen möchten.
2. Wenn Sie Computer in einer Untergruppe der Gruppe prüfen möchten, wählen Sie oben rechts in der Dropdown-Liste **Diese Ebene und abwärts**.
3. Suchen Sie in der Computerliste auf der Registerkarte **Status** die Spalte **On-Access**.

   Wenn in dieser Spalte für den Computer „Aktiv“ angezeigt wird, ist auf dem Computer die On-Access-Scanfunktion aktiviert. Wenn Sie ein graues Schild-Symbol sehen, ist die On-Access-Scanfunktion auf diesem Computer nicht aktiviert.

4. Wenn Sie die Firewall installiert haben, sehen Sie in der Spalte **Firewall aktiviert** nach.

   Wenn dort „Ja“ steht, ist die Firewall aktiviert. Wenn ein graues Firewall-Symbol und ein „Nein“ angezeigt wird, ist die Firewall deaktiviert.

5. Den Status anderer Funktionen (z.B. Application Control, Data Control oder Patch) können Sie in der entsprechenden Spalte einsehen.

Weitere Informationen zum Überprüfen des Computerschutzes finden Sie unter *Überprüfen, ob sich die Computer auf dem neuesten Stand befinden* (Seite 57).

Weitere Informationen zum Auffinden von Computern mit Problemen über Computerlistenfilter finden Sie unter *Auffinden von Computern mit Problemen* (Seite 58).

5.8.4 Überprüfen, ob sich die Computer auf dem neuesten Stand befinden

Wenn Sie Enterprise Console wie empfohlen eingerichtet haben, sollten die Computer automatisch Updates erhalten.

So können Sie feststellen, ob der Computerschutz auf dem neuesten Stand ist:

1. Markieren Sie die Computergruppe, die Sie prüfen möchten.
2. Wenn Sie Computer in einer Untergruppe der Gruppe prüfen möchten, wählen Sie oben rechts in der Dropdown-Liste **Auf dieser Stufe und darunter**.

3. Betrachten Sie auf der Registerkarte **Status** die Spalte **Auf dem neuesten Stand** oder rufen Sie die Registerkarte **Update-Details** auf.
   - Wenn in der Spalte **Auf dem neuesten Stand** „Ja“ steht, befindet sich der Computer auf dem neuesten Stand.
   - Wenn ein Uhrensymbol angezeigt wird, befindet sich der Computer nicht auf dem neuesten Stand. Aus dem Text geht hervor, seit wann sich der Computer nicht mehr auf dem neuesten Stand befindet.

Informationen zum Updaten solcher Computer finden Sie im Abschnitt *Updaten nicht aktueller Computer* (Seite 92).

5.8.5 Überprüfen, ob die Computer verschlüsselt sind

Wenn Sie eine Richtlinie zur **Festplattenverschlüsselung** eingerichtet haben, um Endpoints vor unbefugtem Zugriff zu schützen, sollten die Laufwerke auf den Computern verschlüsselt werden.

So überprüfen Sie, ob die Computer verschlüsselt sind:

1. Markieren Sie die Computergruppe, die Sie prüfen möchten.
2. Wenn Sie Computer in einer Untergruppe der Gruppe prüfen möchten, wählen Sie oben rechts in der Dropdown-Liste **Auf dieser Stufe und darunter**.
3. Betrachten Sie auf der Registerkarte **Status** die Spalte **Vollständige Festplattenverschlüsselung**.

In der Spalte wird der Verschlüsselungsstatus der Computer angezeigt. Die Spalte kann aus folgenden Gründen leer sein:

- Die Verschlüsselungssoftware wurde nicht auf dem Computer installiert.
- Die Verschlüsselungssoftware wurde zwar auf dem Computer installiert, es wurde jedoch noch kein Neustart auf dem Computer durchgeführt. Nach maximal 30 Minuten nach der Installation der Verschlüsselungssoftware werden die Computer automatisch neu gestartet.
- Ein Verschlüsselungsfehler ist aufgetreten.
- Der Computer wird nicht von Sophos Enterprise Console verwaltet.

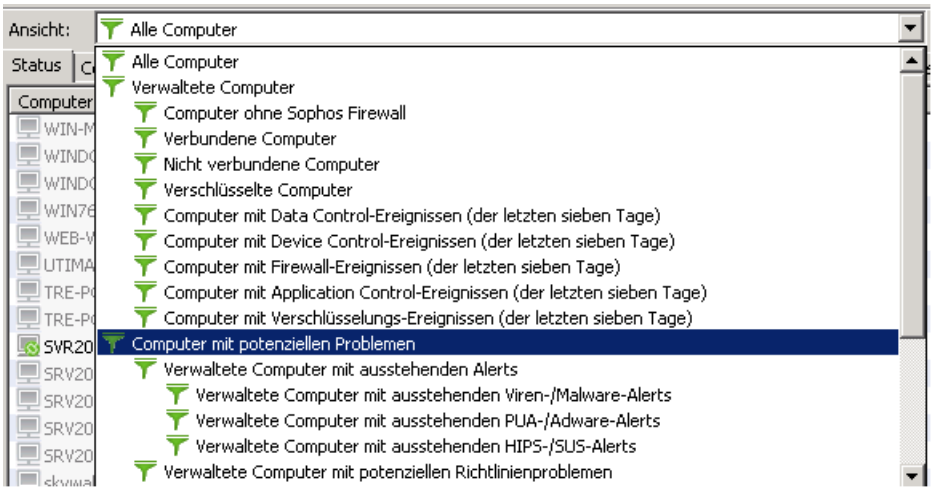
Überprüfen Sie die „Verschlüsselung – Ereignisanzeige“ auf Verschlüsselungsfehler. Fehler werden dort angezeigt.

5.8.6 Auffinden von Computern mit Problemen

So können Sie sich eine Liste der Computer anzeigen lassen, die nicht hinreichend geschützt sind bzw. bei denen Probleme mit dem Computerschutz aufgetreten sind:

1. Markieren Sie die Computergruppe, die Sie prüfen möchten.

2. Wählen Sie im Dropdown-Menü **Ansicht** die gewünschten Computer aus, z.B. **Computer mit potenziellen Problemen**.


Ansicht:
Alle Computer
Status
Computer
Alle Computer
Verwaltete Computer
Computer ohne Sophos Firewall
Verbundene Computer
Nicht verbundene Computer
Verschlüsselte Computer
Computer mit Data Control-Ereignissen (der letzten sieben Tage)
Computer mit Device Control-Ereignissen (der letzten sieben Tage)
Computer mit Firewall-Ereignissen (der letzten sieben Tage)
Computer mit Application Control-Ereignissen (der letzten sieben Tage)
Computer mit Verschlüsselungs-Ereignissen (der letzten sieben Tage)
Computer mit potenziellen Problemen
Verwaltete Computer mit ausstehenden Alerts
Verwaltete Computer mit ausstehenden Viren-/Malware-Alerts
Verwaltete Computer mit ausstehenden PUA-/Adware-Alerts
Verwaltete Computer mit ausstehenden HIPS-/SUS-Alerts
Verwaltete Computer mit potenziellen Richtlinienproblemen

   Sie können außerdem einen untergeordneten Eintrag dieses Eintrags auswählen, um von einem bestimmten Problem betroffene Computer anzuzeigen (z.B. Computer, die von einer Gruppenrichtlinie abweichen, Computer mit ausstehenden Alerts oder Computer, bei denen ein Installationsfehler aufgetreten ist).

3. Wenn die Gruppe auch Untergruppen enthält, wählen Sie, ob Sie Computer **Nur auf dieser Ebene** oder **Diese Ebene und abwärts** suchen möchten.

   Alle Computer mit Schutzproblemen werden aufgelistet.

Anweisungen zum Beheben von Schutzproblemen finden Sie im Abschnitt *Keine Durchführung von On-Access-Scans* (Seite 240) und anderen Themen zur *Fehlersuche*.

5.9 Benachrichtigungen, Alerts und Fehlermeldungen

5.9.1 Was bedeuten die Alert-Symbole?

Wenn ein Virus oder Spyware, ein verdächtiges Objekt, Adware oder eine andere potenziell unerwünschte Anwendung erkannt wird, werden Alert-Symbole in der Ansicht **Endpoints** auf der Registerkarte **Status** angezeigt.

Alerts werden in der folgenden Tabelle erklärt. Die anderen Unterabschnitte bieten Anweisungen zum Umgang mit Alerts.

Hinweis: In der Konsole werden außerdem Warnungen angezeigt, wenn Software deaktiviert wurde oder nicht aktuell ist. Weitere Informationen finden Sie unter *So überprüfen Sie, ob Ihr Netzwerk geschützt ist* (Seite 56).

Alert-Symbole

Symbol	Erklärung
	Ein rotes Warnsymbol in der Spalte **Alerts und Fehler** deutet darauf hin, dass ein Virus, Wurm, Trojaner, Spyware oder verdächtiges Verhalten erkannt wurde.
	Ein gelbes Warnsymbol in der Spalte **Alerts und Fehler** deutet auf eines der folgenden Probleme hin: ■ Eine verdächtige Datei wurde erkannt. ■ Adware oder eine andere potenziell unerwünschte Anwendung wurde erkannt. ■ Ein Fehler ist aufgetreten. Ein gelbes Warnsymbol in der Spalte **Richtlinienkonformität** weist darauf hin, dass die Richtlinie(n) des Computers von den anderen Computern der Gruppe abweichen.

Wenn für einen Computer mehrere Alerts oder Fehler vorhanden sind, wird in der Spalte **Alerts und Fehler** das Symbol des Alerts mit der höchsten Priorität angezeigt. Nachfolgend werden Alert-Typen nach Priorität in absteigender Reihenfolge aufgelistet.

1. Virus-/Spyware-Alert
2. Alerts bei verdächtigem Verhalten
3. Alerts bei verdächtigen Dateien
4. Adware-/PUA-Alerts
5. Software-Anwendungsfehler (beispielsweise Installationsfehler)

Details zu Alerts (z.B. einem erkannten Objekt) finden Sie auf der Registerkarte **Alert- und Fehlerdetails**.

Nähere Informationen zu Update Manager-Allerts finden Sie unter *Übersicht über Update Manager* (Seite 90).

5.9.2 Umgang mit Alerts zu erkannten Objekten

Bei rollenbasierter Verwaltung gilt als Voraussetzung für das Bereinigen von erkannten Objekten bzw. das Löschen von Alerts die Berechtigung **Korrektur – Bereinigung**. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So können Sie die in der Konsole angezeigten Alerts beheben:

1. Markieren Sie in der Ansicht **Endpoints** die Computer, deren Alerts sie anzeigen möchten. Rechtsklicken Sie auf die Auswahl und wählen Sie **Alerts und Fehler löschen** aus.

   Das Dialogfeld **Alerts und Fehler löschen** wird angezeigt.

2. Die zu ergreifende Maßnahme hängt von dem Bereinigungsstatus des Alerts ab. Sehen Sie sich die Spalte **Bereinigungsstatus** an, um zu entscheiden, welche Maßnahme ergriffen werden soll.

Tipp: Sie können auf eine Spaltenüberschrift klicken, um Alerts zu sortieren. So können Sie Alerts etwa nach ihrem **Bereinigungsstatus** sortieren, indem Sie auf die gleichnamige Spaltenüberschrift klicken.

Bereinigungsstatus	Beschreibung und zu ergreifende Maßnahme
Bereinigung möglich	Sie können das Objekt löschen. Wählen Sie hierzu den/die Alert(s) aus und klicken Sie auf **Bereinigung**.
Threat-Typ kann nicht bereinigt werden	Solche erkannten Objekte (z.B. verdächtige Dateien oder verdächtiges Verhalten) lassen sich nicht über die Konsole bereinigen. Sie müssen selbst bestimmen, ob das Objekt zugelassen oder gesperrt werden soll. Sie können Objekte, die Sie nicht als vertrauenswürdig erachten, an Sophos zur Analyse schicken. Nähere Informationen finden Sie unter *Auffinden von Informationen zu erkannten Objekten* (Seite 62).
Keine Bereinigung möglich	Solche Objekte können nicht über die Konsole bereinigt werden. Nähere Informationen zu Objekten und den entsprechenden Gegenmaßnahmen finden Sie unter *Auffinden von Informationen zu erkannten Objekten* (Seite 62).
Vollständige Systemüberprüfung erforderlich	Dieses Objekt kann zwar eventuell bereinigt werden, jedoch nur im Zuge einer vollständigen Systemüberprüfung des Endpoints. Anweisungen hierzu finden Sie unter *Sofort-Scans* (Seite 63).
Neustart erforderlich	Das Objekt wurde teilweise entfernt, die Bereinigung kann jedoch erst nach einem Neustart des Endpoints abgeschlossen werden. **Hinweis:** Endpoints müssen lokal und nicht von Enterprise Console neu gestartet werden.
Bereinigung fehlgeschlagen	Das Objekt konnte nicht entfernt werden. Unter Umständen ist eine manuelle Bereinigung erforderlich. Nähere Informationen finden Sie unter *Bearbeiten erkannter Objekte, falls die Bereinigung fehlschlägt* (Seite 65).
Bereinigung wird durchgeführt (Start <Zeit>)	Bereinigung wird durchgeführt
Zeit für Bereinigung	Zeit für Bereinigung abgelaufen. Das Objekt wurde möglicherweise nicht bereinigt. Dies kann etwa der Fall sein, wenn der Endpoint nicht mit dem

Bereinigungsstatus	Beschreibung und zu ergreifende Maßnahme
abgelaufen (Beginn <Zeit>)	Netzwerk verbunden ist oder das Netzwerk überlastet ist. Sie können versuchen, die Bereinigung zu einem späteren Zeitpunkt zu wiederholen.

Nähere Informationen zum Zulassen von Objekten finden Sie unter *Zulassen von Adware und PUA* (Seite 97) und *Zulassen verdächtiger Objekte* (Seite 107).

5.9.3 Auffinden von Informationen zu erkannten Objekten

Anhand der folgenden Schritte erhalten Sie nähere Informationen zu Threats oder sonstigen auf einem Endpoint erkannten und in der Konsole gemeldeten Objekten sowie zu den zu ergreifenden Gegenmaßnahmen:

1. Doppelklicken Sie in der Ansicht **Endpoints** in der Computerliste auf den betroffenen Computer.
2. Scrollen Sie im Dialogfeld **Computer-Details** zur Option **Ausstehende Alerts und Fehler**. Klicken Sie in der Liste mit den erkannten Objekten auf den Namen des gewünschten Objekts.

   Sie werden mit der Sophos Website verbunden. Hier finden Sie eine Beschreibung des Objekts und Hinweise zu den zu ergreifenden Gegenmaßnahmen.

Hinweis: Sie können jedoch auch die **Sicherheitsanalysen** auf der Sophos Website aufrufen (*http://www.sophos.de/security/analyses/*). Klicken Sie auf die Registerkarte des gewünschten Objekttyps, geben Sie den Namen des Objekts in das Suchfeld ein oder suchen Sie es in der Objektliste.

5.9.4 Löschen von Endpoint-Alerts und -Fehlern über die Konsole

Bei rollenbasierter Administration gilt als Voraussetzung für das Löschen von Alerts und Fehlern die Berechtigung **Korrektur – Bereinigung**. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wenn Sie Maßnahmen bei Alerts ergreifen oder wissen, dass der Computer sicher ist, können Sie das in der Konsole angezeigte Alert-Symbol löschen.

Hinweis: Alerts zu Installationsfehlern lassen sich nicht löschen. Alerts lassen sich nur löschen, wenn Sophos Endpoint Security and Control auf dem Computer installiert ist.

1. Markieren Sie in der Ansicht **Endpoints** die Computer, für die Sie Alerts löschen möchten. Rechtsklicken Sie auf die Auswahl und wählen Sie **Alerts und Fehler löschen** aus.

   Das Dialogfeld **Alerts und Fehler löschen** wird angezeigt.

2. Rufen Sie zum Löschen von Alerts oder Fehlermeldungen bei Sophos Produkten die Registerkarte „Alerts“ bzw. „Fehler“ auf, wählen Sie die gewünschten Alerts/Fehler aus und klicken Sie auf **Löschen**.

   Gelöschte Alerts werden nicht mehr in der Konsole angezeigt.

Weitere Informationen zum Löschen von Update Manager-Alerts aus der Konsole finden Sie unter *Löschen von Update Manager-Alerts aus der Konsole* (Seite 91).

5.10 Scannen von Computern

5.10.1 Scan-Informationen

Standardmäßig erkennt Sophos Endpoint Security and Control bekannte und unbekannte Viren, Trojaner, Würmer und Spyware automatisch, wenn ein Benutzer versucht, auf Dateien zuzugreifen, in denen sie enthalten sind. Außerdem wird das Verhalten der Programme analysiert, die auf dem System laufen.

Ferner können Sie die folgenden Einstellungen in Sophos Endpoint Security and Control vornehmen:

- Scannen von Computern auf verdächtige Dateien. Mehr dazu erfahren Sie unter *Scannen auf verdächtige Dateien im Rahmen von On-Access-Scans* (Seite 102).
- Scannen auf Adware und potenziell unerwünschte Anwendungen. Mehr dazu erfahren Sie unter *Scannen auf Adware und PUA* (Seite 96).
- Scannen von Computern zu festen Zeiten. Mehr dazu erfahren Sie unter *Scannen von Computern zu bestimmten Zeiten* (Seite 108).

Weitere Informationen zur Konfiguration von Scans entnehmen Sie bitte dem Abschnitt *Die Antivirus- und HIPS-Richtlinie* (Seite 94).

In diesem Abschnitt wird beschrieben, wie eine vollständige Systemüberprüfung ausgewählter Computer sofort durchgeführt werden kann.

5.10.2 Sofort-Scans

Sie können einen oder mehrere Computer sofort scannen, ohne auf den nächsten geplanten Scan warten zu müssen.

Bei rollenbasierter Verwaltung müssen Sie zum Updaten von Computern über die Berechtigung **Korrektur – Updates und Scans** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Hinweis: Sofortige vollständige Systemüberprüfungen über die Konsole sind nur unter Windows 2000 oder höher und UNIX möglich.

So werden Computer sofort gescannt:

1. Wählen Sie den Computer in der Computer-Liste oder eine Gruppe im Fensterbereich **Gruppen**. Rechtsklicken Sie darauf und wählen Sie **Vollständige Systemüberprüfung**.

   Sie können aber auch im Menü **Maßnahmen** die Option **Vollständige Systemüberprüfung** wählen.

2. Wenn all Angaben im Dialogfeld **Vollständige Systemüberprüfung** richtig sind, klicken Sie auf **OK**, um die Überprüfung zu starten.

Hinweis: Wenn beim Scan Threat-Komponenten im Speicher erkannt werden, wird der Scan angehalten und ein Alert wird an Enterprise Console gesendet. Wenn der Scan fortgesetzt wird, könnte sich der Threat ausbreiten. Sie müssen den Threat zunächst bereinigen, bevor Sie den Scan erneut ausführen können.

5.11 Bereinigen von Computern

5.11.1 Sofortiges Bereinigen von Computern

Computer unter Windows 2000 und höher oder Mac, auf denen sich ein Virus oder unerwünschte Anwendungen befinden, können sofort bereinigt werden.

Bei rollenbasierter Verwaltung müssen Sie zur Bereinigung über die Berechtigung **Korrektur – Bereinigung** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Hinweis: Zur Bereinigung von Linux- oder UNIX-Systemen können Sie entweder anhand der Anweisungen im Abschnitt *Einrichten der automatischen Bereinigung für On-Access-Scans* (Seite 65) eine automatische Bereinigung von der Konsole aus einrichten oder die Computer einzeln bereinigen, wie unter *Bearbeiten erkannter Objekte, falls die Bereinigung fehlschlägt* (Seite 65) beschrieben.

Wenn ein Objekt (z.B. ein Trojaner oder eine potenziell unerwünschte Anwendung) vor der Bereinigung des betroffenen Computers „teilweise erkannt“ wurde, führen Sie eine vollständige Systemüberprüfung durch, um alle Komponenten des erkannten Objektfragments aufzufinden. Wechseln Sie in der Computerliste in die Ansicht **Endpoints**, rechtsklicken Sie auf den betroffenen Computer und klicken Sie auf **Vollständige Systemüberprüfung**. Nähere Informationen finden Sie unter *Zum Teil erkanntes Objekt* (Seite 244).

So können Sie Ihre Computer sofort bereinigen:

1. Wechseln Sie in der Computerliste in die Ansicht **Endpoints**, rechtsklicken Sie auf den/die zu bereinigenden Computer und wählen Sie **Alerts und Fehler löschen**.
2. Wählen Sie im Dialogfeld **Alerts und Fehler löschen** die Registerkarte **Alerts**. Aktivieren Sie das Kontrollkästchen neben allen Objekten, die Sie bereinigen möchten oder klicken Sie auf **Alles markieren**. Klicken Sie auf **Bereinigung**.

Wenn die Bereinigung erfolgreich war, werden die Alerts der Computerliste nicht mehr angezeigt.

Wenn weiterhin Alerts vorhanden sind, sollten Sie die Computer manuell bereinigen. Mehr dazu erfahren Sie unter *Bearbeiten erkannter Objekte, falls die Bereinigung fehlschlägt* (Seite 65).

Hinweis: Bei der Bereinigung wird unter Umständen eine vollständige Systemüberprüfung auf den betroffenen Computern eingeleitet, um *alle* Viren zu bereinigen. Dieser Vorgang kann viel Zeit in Anspruch nehmen. Die Alerts werden nach Abschluss des Scan-Vorgangs aktualisiert.

5.11.2 Bearbeiten erkannter Objekte, falls die Bereinigung fehlschlägt

Wenn Sie Computer nicht von der Konsole aus bereinigen können, führen Sie die Bereinigung manuell durch:

1. Doppelklicken Sie in der Computerliste auf den infizierten Computer.
2. Scrollen Sie im Dialogfeld **Computer-Details** zur Option **Ausstehende Alerts und Fehler**. Klicken Sie in der Liste mit den erkannten Objekten auf das Objekt, das Sie entfernen möchten.

   Eine Verbindung zur Sophos Website wird hergestellt; hier finden Sie Tipps zur Bereinigung des Computers.

3. Gehen Sie zu dem Computer und führen Sie die Bereinigung manuell durch.

   Hinweis: Auf der Sophos Website stehen außerdem spezielle Desinfektions-Tools für bestimmte Viren und Würmer zum Download bereit.

5.11.3 Einrichten der automatischen Bereinigung für On-Access-Scans

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Standardmäßig bereinigt Sophos Endpoint Security and Control Computer automatisch bei Erkennen von Viren oder sonstigen Threats. Sie können die Einstellungen der automatischen Bereinigung anhand der Anweisungen unten ändern.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**.
3. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.

4. Klicken Sie im Feld **On-Access-Scans** neben **On-Access-Scans aktivieren** auf **Konfigurieren**.
5. Klicken Sie im Dialogfeld **Einstellungen für On-Access-Scans** auf die Registerkarte **Bereinigung**.
6. Legen Sie die Option in Einklang mit den Anweisungen in Abschnitt *Einstellungen der automatischen Bereinigung für On-Access-Scans* (Seite 66) fest.

5.11.4 Einstellungen der automatischen Bereinigung für On-Access-Scans

Viren/Spyware

Aktivieren/deaktivieren Sie die Option **Objekte mit Virus/Spyware automatisch bereinigen**.

Sie können außerdem festlegen, was mit den Objekten geschehen soll, falls die Bereinigung fehlschlägt:

Zugriff verweigern
Löschen
Zugriff verweigern und in das Standardverzeichnis verschieben
Zugriff verweigern und verschieben nach (vollständiger UNC-Pfad)

Hinweis: Die gewählten Optionen im Bereich **Zugriff verweigern und in den Standardspeicherort verschieben** und **Zugriff verweigern und in Standardverzeichnis verschieben** werden auf Linux- oder UNIX-Computern ignoriert.

Verdächtige Dateien

Hinweis: Diese Einstellungen gelten nur für Systeme unter Windows 2000 und aufwärts.

Sie können festlegen, was mit verdächtigen Dateien geschehen soll, wenn sie erkannt werden:

Zugriff verweigern
Löschen
Zugriff verweigern und in das Standardverzeichnis verschieben
Zugriff verweigern und verschieben nach (vollständiger UNC-Pfad)

5.11.5 Einrichten der automatischen Bereinigung für geplante Scans

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Standardmäßig bereinigt Sophos Endpoint Security and Control Computer automatisch bei Erkennen von Viren oder sonstigen Threats. Sie können die Einstellungen der automatischen Bereinigung anhand der Anweisungen unten ändern.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**.
3. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.
4. Wählen Sie im Dialogfeld **Geplante Scans** den Scan aus und klicken Sie auf **Bearbeiten**.
5. Klicken Sie neben **Einstellungen zu Scans und Bereinigung ändern** auf **Konfigurieren**.

   Das Dialogfeld **Scan- und Bereinigungs-Einstellungen** wird geöffnet.
6. Klicken Sie auf die Registerkarte **Bereinigung**.
7. Legen Sie die Option in Einklang mit den Anweisungen in Abschnitt *Einstellungen der automatischen Bereinigung für geplante Scans* (Seite 67) fest.

5.11.6 Einstellungen der automatischen Bereinigung für geplante Scans

Viren/Spyware

Aktivieren/deaktivieren Sie die Option **Objekte mit Virus/Spyware automatisch bereinigen**.

Sie können außerdem festlegen, was mit den Objekten geschehen soll, falls die Bereinigung fehlschlägt:

Nur protokollieren
Löschen
In Standardspeicherort verschieben
Verschieben nach (vollständiger UNC-Pfad)

Hinweise

- Das Verschieben einer ausführbaren Datei senkt das Risiko, dass diese Datei gestartet wird.
- Eine Infektion mit mehreren Komponenten kann nicht automatisch verschoben werden.

Adware und PUA

Wählen Sie die Option **Adware und PUA automatisch bereinigen**.

Hinweis

- Diese Einstellung ist nur für Windows 2000 und höher relevant.

Verdächtige Dateien

Sie können festlegen, was mit verdächtigen Dateien geschehen soll, wenn sie erkannt werden:

Nur protokollieren
Löschen
In Standardspeicherort verschieben
Verschieben nach (vollständiger UNC-Pfad)

Hinweise

- Diese Einstellungen gelten nur für Systeme unter Windows 2000 und aufwärts.
- Das Verschieben einer ausführbaren Datei senkt das Risiko, dass diese Datei gestartet wird.
- Eine Infektion mit mehreren Komponenten kann nicht automatisch verschoben werden.

6 Updates

6.1 Konfigurieren des Update Managers

6.1.1 Wozu dient ein Update Manager?

Mit einem Update Manager können Sie automatische Updates von Sophos Sicherheitssoftware über die Sophos Website konfigurieren. Der Update Manager wird mit Enterprise Console installiert und verwaltet.

Hinweis: Updates der Verschlüsselungssoftware erfolgen über den Assistenten zum Schutz von Computern. Nähere Informationen hierzu finden Sie unter *Automatische Installation von Verschlüsselungssoftware* (Seite 53).

Sie können mehrere Update Manager installieren. Wenn Ihr Unternehmensnetzwerk beispielsweise mehrere Standorte umfasst, empfiehlt sich, einen zusätzlichen Update Manager an einem Remote-Standort zu installieren. Nähere Informationen hierzu finden Sie unter *Hinzufügen eines weiteren Update Managers* (Seite 75).

6.1.2 Funktionsweise eines Update Managers

Nach der Konfiguration führt der Update Manager die folgenden Aufgaben aus:

- Er stellt in regelmäßigen Abständen eine Verbindung zu einem Datenverteilungs-Warehouse bei Sophos bzw. in Ihrem Netzwerk her.
- Er lädt Updates für Threat-Erkennungsdaten und für Sicherheitssoftware herunter, die der Administrator abonniert hat.
- Er legt die Software-Updates in installierbarer Form in einer oder mehreren Netzwerkfreigaben ab.

Die Computer laden Updates automatisch aus den Freigaben herunter, sofern die installierte Software entsprechend konfiguriert wurde (z.B. durch Übertragen einer Update-Richtlinie).

6.1.3 Anzeigen oder Ändern der Update Manager-Konfiguration

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren eines Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.

2. Wählen Sie den Update Manager, dessen Konfiguration angezeigt oder geändert werden soll, in der Liste aus. Rechtsklicken Sie darauf und klicken Sie auf **Konfiguration**.

   Hinweis: Sie können jedoch auch wie folgt verfahren: Rufen Sie das Menü **Maßnahmen** auf, richten Sie den Mauszeiger auf **Update Manager** und klicken Sie anschließend auf **Konfiguration**.

   Das Dialogfenster **Update Manager konfigurieren** wird angezeigt.

3. Anweisungen zum Ändern der Konfigurationseinstellungen entnehmen Sie bitte den folgenden Abschnitten.

   - *Auswahl einer Update-Quelle für einen Update Manager* (Seite 70).
   - *Softwareauswahl* (Seite 71).
   - *Festlegen des Download-Verzeichnisses* (Seite 72).
   - *Erstellen/Ändern eines Update-Zeitplans* (Seite 73).
   - *Konfigurieren des Update Manager-Protokolls* (Seite 74).
   - *Konfigurieren der Selbst-Update-Funktion von Update Managern* (Seite 74).

Weitere Informationen zum Löschen von Update Manager-Alerts aus der Konsole finden Sie unter *Löschen von Update Manager-Alerts aus der Konsole* (Seite 91).

Wenn Sie den Update Manager konfiguriert haben, können Sie Ihre Update-Richtlinie konfigurieren und sie auf die Endpoints übertragen.

6.1.4 Auswahl einer Update-Quelle für einen Update Manager

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren eines Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie müssen eine Quelle auswählen, von der ein Update Manager Sicherheitssoftware und Updates herunterlädt, die im Netzwerk verteilt werden.

Sie können mehrere Quellen angeben. Bei der ersten Quelle handelt es sich um die Primärquelle. Die übrigen Quellen in der Liste können auf Wunsch für den Fall angegeben werden, dass der Update Manager nicht auf die Primärquelle zugreifen kann.

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie aus der Update Manager-Liste den Update-Manager aus, dem eine Quelle zugewiesen werden soll. Rechtsklicken Sie darauf und klicken Sie auf **Konfiguration**.
3. Klicken Sie im Fenster **Update Manager konfigurieren** auf der Registerkarte **Quellen** auf die Option **Hinzufügen**.
4. Geben Sie in das Dialogfeld **Quellenangaben** die Adresse der Quelle in das **Adress**-Feld ein. Es kann sich bei der Adresse um einen UNC- oder einen HTTP-Pfad handeln.

   Wenn Sie Software und Updates direkt von Sophos herunterladen möchten, wählen Sie **Sophos**.

5. Geben Sie bei Bedarf den **Benutzernamen** und das **Kennwort** für den Zugriff auf die Update-Quelle in die entsprechenden Felder ein.

   - Wenn die Update-Quelle „Sophos“ lautet, geben Sie die Download-Zugangsdaten ein, die Sie von Sophos erhalten haben.
   - Wenn es sich bei der Update-Quelle um die von einem Update Manager einer höheren Hierarchieebene erstellte Standard-Update-Quelle handelt, sind die Felder **Benutzername** und **Kennwort** bereits ausgefüllt.

     Die Standard-Update-Freigabe ist eine UNC-Freigabe: \\<ComputerName>\SophosUpdate. ComputerName steht dabei für den Namen des Computers, auf dem der Update Manager installiert wurde.
   - Wenn Sie nicht auf einen Standard-Update-Quelle im Netzwerk zugreifen, geben Sie die Zugangsdaten des Kontos ein, das Lesezugriff auf die Freigabe besitzt. Falls der **Benutzername** auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.

6. Wenn Sie auf die Update-Quelle über einen Proxyserver zugreifen, wählen Sie die Option **Über Proxyserver verbinden**. Geben Sie anschließend die **Adresse** und den **Port** des Proxyservers an. Geben Sie die **Zugangsdaten** des Proxyservers ein. Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein. Klicken Sie auf „OK“.

   Die neue Quelle wird in der Liste im Dialogfeld **Update Manager konfigurieren** angezeigt.

Wenn Sie bereits einen Update Manager auf einem anderen Computer installiert haben, erscheint die die Freigabe, von der der Update Manager Software und Updates bezieht, in der Adressenliste. Sie können die Freigabe als Quelle für den Update Manager angeben, den Sie konfigurieren. Anschließend können Sie die gewünschte Primäradresse mit Hilfe der Pfeilschaltflächen rechts neben der Liste ganz nach oben verschieben.

6.1.5 Softwareauswahl

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren eines Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie müssen die Abonnements auswählen, die der Update Manager auf dem neuesten Stand halten soll.

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie den gewünschten Update Manager aus der Liste aus. Rechtsklicken Sie darauf und klicken Sie auf **Konfiguration**.
3. Rufen Sie im Dialogfeld **Update Manager konfigurieren** die Registerkarte **Abonnements** auf und wählen Sie ein Abonnement aus der Liste mit den vorhandenen Abonnements aus.

   Details zum Abonnement (z.B. vom Abonnement erfasste Software) können Sie per Klick auf **Details** aufrufen.

4. Klicken Sie zum Verschieben des gewählten Abonnements in die Liste „Abonniert für“ auf die Schaltfläche „Hinzufügen“.

   Klicken Sie auf „Alle hinzufügen“, wenn Sie alle Abonnements in die Liste „Abonniert für“ verschieben möchten.

6.1.6 Festlegen des Download-Verzeichnisses

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren eines Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wenn Sie angegeben haben, welche Software heruntergeladen werden soll, können Sie nun das Download-Verzeichnis im Netzwerk angeben. Standardmäßig wird Software in einer UNC-Freigabe abgelegt: \\<Computername>\SophosUpdate. ComputerName steht dabei für den Namen des Computers, auf dem der Update Manager installiert wurde.

Sie können heruntergeladene Software in weiteren Freigaben im Netzwerk bereitstellen. Nehmen Sie hierzu eine vorhandene Netzwerkfreigabe in die Liste der verfügbaren Freigaben auf und verschieben Sie sie von dort anhand der folgenden Anweisungen in die Liste der Update-Freigaben. Stellen Sie sicher, dass das **SophosUpdateMgr**-Konto über Lesezugriff auf die Freigaben verfügt.

Im Abschnitt *Unterstützte Netzwerkfreigaben* (Seite 73) können Sie nachlesen, welche Systeme unterstützt werden.

So legen Sie das Download-Verzeichnis fest:

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie den gewünschten Update Manager aus der Liste aus. Rechtsklicken Sie darauf und klicken Sie auf **Konfiguration**.
3. Wählen Sie im Dialogfeld **Update Manager konfigurieren** auf der Registerkarte **Verteilung** ein Software-Abonnement aus der Liste aus.
4. Wählen Sie eine Freigabe aus der Liste der verfügbaren Freigaben aus und verschieben Sie sie durch Klicken auf die Schaltfläche „Hinzufügen“ (>) in die Liste „Update auf“.

   Die Standardfreigabe \\<Computername>\SophosUpdate befindet sich immer in der Liste „Update auf“. Die Freigabe kann nicht gelöscht werden.

   Die Liste der verfügbaren Freigaben umfasst alle Freigaben, die Enterprise Console bekannt sind und nicht bereits von einem anderen Update Manager genutzt werden.

   Über die Schaltfläche „Hinzufügen“ (>) bzw. „Entfernen“ (<) können Sie Freigaben in die Liste der verfügbaren Freigaben aufnehmen oder aus der Liste entfernen.

5. Wenn Sie eine Beschreibung zu einer Freigabe oder Zugangsdaten zum Schreiben in die Freigabe angeben möchten, wählen Sie die Freigabe aus und klicken Sie auf **Konfigurieren**. Geben Sie im Dialogfeld **Freigaben-Manager** die Beschreibung und die Zugangsdaten ein.

   Wenn Sie die gleichen Zugangsdaten für mehrere Freigaben eingeben möchten, wählen Sie die Freigaben in der Liste Update auf aus und klicken Sie auf **Konfigurieren**. Geben Sie in das Dialogfeld **Mehrere Freigaben konfigurieren** die Zugangsdaten zum Schreiben auf die Freigaben ein.

6.1.7 Unterstützte Netzwerkfreigaben

Netzwerkfreigaben der folgenden Betriebssysteme werden unterstützt:

- Freigaben in Windows NT und höher.
- Auf Linux-Servern gehostete Samba-Freigaben, z.B. SUSE Linux Enterprise 10 (SLES 10).
- Auf Netware 5.1 SP3- und Netware 6.5 SP3- bis SP7-Kerneln gehostete Samba-Freigaben.
- Auf Mac OSX 10.2 und höher gehostete Samba-Freigaben.
- Auf Unix gehostete Samba-Freigaben.
- Novell Storage Services (NSS)-Freigaben mit NDS-Authentifizierung, gehostet auf Novell Open Enterprise Server 1 und 2, Linux-Kernel.
- Netware File System (NFS)-Freigaben mit NDS-Authentifizierung, gehostet auf Netware 5.1 SP3 und Netware 6.5 SP3 bis SP7, Netware-Kernel.
- NetApp Filer.
- Auf Novell Open Enterprise Server 1 und 2 gehostete Samba-Freigaben.
- Novell Storage Services (NSS)-Freigaben, mit NDS-Authentifizierung, gehostet auf Netware 5.1 SP3 und Netware 6.5 SP3 bis SP7, Netware-Kernel.

6.1.8 Erstellen/Ändern eines Update-Zeitplans

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren eines Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Standardmäßig sucht ein Update Manager alle 10 Minuten in der Sophos Datenbank nach Updates für Threat-Erkennungsdaten.

Sie können das Update-Intervall ändern. Das Intervall muss mindestens 5 und höchstens 1440 Minuten (24 Stunden) betragen. Es empfiehlt sich ein Update-Intervall von 10 Minuten für Threat-Erkennungsdaten, um sicherzustellen, dass Sie umgehend vor neu erkannten Threats geschützt sind.

Standardmäßig sucht der Update Manager alle 60 Minuten in der Sophos Datenbank nach **Software**-Updates.

Sie können das Update-Intervall ändern. Das Intervall muss mindestens 10 und höchstens 1440 Minuten (24 Stunden) betragen.

Als Update-Intervall ist etwa „stündlich an allen Tagen“ denkbar. Sie können jedoch auch komplexere Zeitpläne erstellen und etwa unterschiedliche Update-Zeiträume für unterschiedliche Tage festlegen.

Hinweis: Sie können unterschiedliche Zeitpläne für alle Tage festlegen. Jedem Wochentag kann jeweils nur ein Zeitplan zugeordnet werden.

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie aus der Update Manager-Liste den Update-Manager aus, für den ein Zeitplan erstellt werden soll. Rechtsklicken Sie darauf und klicken Sie auf **Konfiguration**.
3. Rufen Sie im Dialogfeld **Update Manager konfigurieren** die Registerkarte **Zeitplan** auf und legen Sie ein Intervall für Threat-Erkenunngdsdaten fest.
4. Geben Sie ein Intervall für Software-Updates ein.
   - Wenn Sie ein Update-Intervall für alle Stunden festlegen möchten, wählen Sie die Option **Auf Updates prüfen alle n Minuten** und geben Sie ein Intervall in Minuten an.
   - Wenn Sie einen komplexeren Zeitplan wünschen oder den einzelnen Wochentagen unterschiedliche Zeitpläne zuweisen möchten, wählen Sie die Option **Geplante Updates einrichten und verwalten** aus und klicken Sie anschließend auf **Hinzufügen**.

     Geben Sie in das Dialogfeld **Update-Zeitplan** einen Namen für den Zeitplan ein und wählen Sie die Wochentage und Update-Intervalle aus.

6.1.9 Konfigurieren des Update Manager-Protokolls

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren eines Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie aus der Update Manager-Liste den Update-Manager aus, für den ein Protokoll erstellt werden soll. Rechtsklicken Sie darauf und klicken Sie auf **Konfiguration**.
3. Geben Sie im Dialogfeld **Update Manager konfigurieren** auf der Registerkarte **Protokolle** an, wie lange das Protokoll gespeichert werden soll, und wählen Sie die Maximalgröße des Protokolls aus.

6.1.10 Konfigurieren der Selbst-Update-Funktion von Update Managern

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren eines Update Managers über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie aus der Update Manager-Liste den Update-Manager aus, dessen Updates konfiguriert werden sollen. Rechtsklicken Sie darauf und klicken Sie auf **Konfiguration**.

3. Wählen Sie im Dialogfeld **Update Manager konfigurieren** auf der Registerkarte **Erweitert** die gewünschte Update Manager-Version aus.
   Wenn Sie beispielsweise die Option „empfohlen“ auswählen, wird der Update Manager stets an die Version mit der entsprechenden Bezeichnung angepasst. Die Version des Update Managers ändert sich dabei.

6.1.11 Sofort-Update-Suche

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Korrektur – Updates und Scans** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Nach der Konfiguration sucht der Update Manager nach vorhandenen Updates und lädt sie in Einklang mit dem festgelegten Zeitplan von der Update-Quelle in die automatisch verwalteten Update-Freigaben herunter. Wenn der Update Manager sofort nach Threat-Detection-Daten-Updates, Software-Updates für Endpoints sowie Software-Updates für den Update Manager selbst suchen soll, verfahren Sie wie folgt:

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie aus der Update Manager-Liste den Update-Manager aus, der upgedatet werden soll. Rechtsklicken Sie darauf und wählen Sie **Jetzt updaten**.

6.1.12 Übernahme der Konfigurationseinstellungen

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Korrektur – Updates und Scans** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Wählen Sie den Update Manager aus der Liste aus, für den die Einstellungen übernommen werden sollen. Rechtsklicken Sie auf die Auswahl und wählen Sie **Konformität mit Konfiguration**.

6.1.13 Hinzufügen eines weiteren Update Managers

Sophos Update Manager (SUM) wird immer auf dem Computer installiert, auf dem sich auch Enterprise Console befindet. Wenn Sie sich bei der Installation für das **Benutzerdefinierte Setup** entschieden haben, befindet sich auf diesem Computer auch der Management-Server.

Sie können einen oder mehrere Update Manager in Ihr Netzwerk aufnehmen. So wird der installierte Update Manager entlastet und Updates werden effektiver installiert. Sie können zusätzliche Update Manager auf einem Computer installieren, auf dem sich noch kein Update Manager befindet.

Wichtig: Entfernen Sie nicht den Update Manager, der sich auf dem selben Computer wie der Management-Server von Enterprise Console befindet. Enterprise Console kann das Netzwerk nicht vollständig schützen, bis für den Update Manager eine Update-Quelle

eingerichtet wurde. Enterprise Console empfängt dann die erforderlichen Updates (Informationen zu den empfohlenen Sicherheitssoftware-Versionen, neue und aktualisierte Content Control Lists für Data Control oder die aktualisierte Liste überwachter Geräte und Anwendungen).

Öffnen Sie auf dem Computer, auf dem ein weiterer Update Manager installiert werden soll, Port 80, damit der zusätzliche Update Manager Sicherheitssoftware von Sophos oder einem anderen Update Manager über HTTP herunterladen kann. Öffnen Sie die Ports 137, 138, 139 und 445 auf dem Computer, damit der Update Manager Sicherheitssoftware von einem anderen Update Manager über einen UNC-Pfad herunterladen kann.

Wenn die Windows-Version des Computers über integrierte Netzwerkerkennung verfügt, diese Funktion jedoch deaktiviert ist, aktivieren Sie sie und starten Sie den Computer neu.

Wenn der Computer unter Windows Server 2008 betrieben wird, deaktivieren Sie die Benutzerkontensteuerung und starten Sie den Computer neu. Nach der Installation des Update Managers und der Anmeldung für die Sophos Updates können Sie die Benutzerkontensteuerung wieder aktivieren.

Wenn der Computer unter Windows 2000 betrieben wird, muss er nach der Installation neu gestartet werden.

Wenn sich der Computer in einer Domäne befindet, melden Sie sich als Domänenadministrator an.

Wenn sich der Computer in einer Arbeitsgruppe befindet, melden Sie sich als lokaler Administrator an.

Der Update Manager-Installer befindet sich in der Freigabe (\\Servername\SUMInstallSet) auf dem Computer, auf dem der Management-Server von Enterprise Console installiert ist. Sie können sich das Verzeichnis, in dem sich der Installer befindet, anzeigen lassen: Rufen Sie das Menü **Ansicht** auf und klicken Sie auf **Sophos Update Manager-Verzeichnis**.

Sie können den Sophos Update Manager über die Remotedesktop-Funktion von Windows installieren.

So können Sie weitere Update Manager installieren:

1. Führen Sie den Sophos Update Manager-Installer **Setup.exe** aus.

   Ein Installations-Assistent öffnet sich.

2. Klicken Sie im Startbildschirm des Assistenten auf **Weiter**.
3. Lesen Sie die **Lizenzvereinbarung**. Wenn Sie mit den Bedingungen einverstanden sind, klicken Sie auf **Ich stimme den Bedingungen des Lizenzvertrags zu**. Klicken Sie auf **Weiter**.
4. Übernehmen Sie den Standardzielordner auf der Seite **Zielordner** oder klicken Sie auf **Ändern** und geben Sie einen neuen Zielordner an. Klicken Sie auf **Weiter**.

5. Wählen Sie auf der Seite **Sophos Update Manager-Konto** ein Konto aus, über das Endpoints auf die vom Update Manager erstellte Standard-Update-Freigabe zugreifen können. Die Standard-Update-Freigabe lautet \\<ComputerName>\SophosUpdate. ComputerName steht dabei für den Namen des Computers, auf dem der Update Manager installiert wurde. Das Konto muss Lesezugriff auf die Freigabe haben. Administratorrechte sind jedoch nicht erforderlich.

   Sie können den Standardbenutzer oder einen vorhandenen Benutzer auswählen oder einen neuen Benutzer erstellen.

   Standardmäßig weist der Installer dem **SophosUpdateMgr**-Konto Lesezugriff auf die Update-Freigabe, jedoch keine interaktiven Anmelderechte zu.

   Wenn Sie später weitere Update-Freigaben hinzufügen möchten, wählen Sie ein vorhandenes Konto oder erstellen Sie ein neues Konto, das mit Lesezugriffsrechten an den Freigaben ausgestattet ist. Stellen Sie ansonsten sicher, dass das **SophosUpdateMgr**-Konto über Lesezugriff auf die Freigaben verfügt.

6. Geben Sie auf der Seite **Kontodetails zu Sophos Update Manager** in Abhängigkeit von der auf der vorherigen Seite gewählten Option das Kennwort des Standardbenutzers oder die Kontodaten des neuen Benutzers ein oder wählen Sie ein vorhandenes Konto aus.

   Das Kennwort des Kontos muss Ihrer Kennwortrichtlinie entsprechen.

7. Klicken Sie im Dialogfeld **Das Programm kann jetzt installiert werden** auf die Option **Installieren**.
8. Klicken Sie nach Abschluss der Installation auf **Fertigstellen**.

Der Computer, auf dem Sophos Update Manager installiert wurde, wird nun in Enterprise Console in der Ansicht **Update Manager** angezeigt. Klicken Sie im Menü **Ansicht** auf **Update Manager**.

Wählen Sie den Update Manager zur Konfiguration aus, rechtsklicken Sie darauf und klicken Sie anschließend auf **Konfiguration**.

6.1.14 Freigeben von Sicherheitssoftware in einem Webserver

Bisweilen empfiehlt sich, Sophos Sicherheitssoftware in einem Webserver freizugeben, damit Computer über HTTP darauf zugreifen können. Bei der Installation von Sophos Anti-Virus für UNIX, Version 4, Sophos Anti-Virus für UNIX dieser Schritt durchgeführt werden, kann jedoch auf Wunsch auch erst nach dem Download von Sophos Anti-Virus für UNIX, Version 4, erfolgen.

So geben Sie Sicherheitssoftware in einem Webserver frei:

1. Den Pfad zur Freigabe, in die die Sicherheitssoftware heruntergeladen wurde („Bootstrap-Verzeichnis“), können Sie wie folgt ermitteln:

   a) Klicken Sie in Enterprise Console, im Menü **Ansicht** auf **Bootstrap-Verzeichnisse**.

      Im Dialogfeld **Bootstrap-Verzeichnisse** werden in der Spalte **Verzeichnis** die Bootstrap-Verzeichnisse für alle Plattformen angezeigt.

   b) Notieren Sie sich den Pfad bis ausschließlich des Ordners des zentralen Installationsverzeichnisses. Beispiel:
      server name\SophosUpdate

2. Stellen Sie das Bootstrap-Verzeichnis, einschließlich der Unterordner, auf dem Webserver bereit.
3. Legen Sie Benutzernamen und Kennwörter zum Schutz vor unerlaubtem Zugriff auf den Ordner im Webserver fest.

   Die Komponente „Sophos AutoUpdate“ von Sophos Endpoint Security and Control unterstützen die folgenden HTTP-Authentifizierungsarten:

   - Basis
   - NTLM (Version 1 und Version 2)
   - Digest (auf manchen Webservern kann AutoUpdate keine Updates mit Digest-Authentifizierung durchführen)

   Wir empfehlen eine sichere Option (d.h. NTLM 2) zur Konfiguration der Unternehmens-Website für Sophos-Updates.

Anweisungen zur Freigabe von Ordnern im Internet und zum Einrichten von Zugangsdaten entnehmen Sie bitte dem Begleitmaterial des Webservers. Wenden Sie sich bei weiteren Fragen bitte an Ihren Webserver-Betreiber.

Internetinformationsdienste (IIS) und Sophos Software

Wenn Sie Version 6.0 der Internetinformationsdienste (IIS) (mit Windows 2003 mitgeliefert) verwenden, werden nur Dateien, deren Erweiterung in der MIME-Typen-Liste der IIS registriert ist, verarbeitet. Um sicherzustellen, dass IIS Sophos-Dateien berücksichtigt, fügen Sie alle Erweiterungen der Dateien zur Liste hinzu (oder arbeiten Sie mit Platzhaltern '.*'): Suchen Sie hierzu das Sophos Verzeichnis auf der obersten Ebene auf und klicken Sie auf **Eigenschaften**. Klicken Sie im Dialogfeld **Eigenschaften der Website** auf die Registerkarte **HTTP-Header**. Wählen Sie anschließend die Option „MIME-Typen“ aus und fügen Sie die Erweiterungen hinzu. Weisen Sie sie dem MIME-Typ „Application/Octet-Stream“ zu.

Wenn Sie die IIS mit anonymer Authentifizierung verwenden und den Webserver als primären Update-Server in der Update-Richtlinie verwenden möchten, müssen Sie die Zugangsdaten für den primären Server in der Update-Richtlinie eingeben. Andernfalls können Sie die Endpointes nicht über die Konsole schützen. Mehr dazu erfahren Sie unter *Ändern der Zugangsdaten zum Primärserver* (Seite 86).

6.2 Konfigurieren von Software-Abonnements

6.2.1 Software-Abonnements

Durch Software-Abonnements wird festgelegt, welche Endpoint-Softwareversionen für die jeweiligen Plattformen von Sophos heruntergeladen werden.

Der **Download-Assistent für Sicherheitssoftware** richtet ein Standardabonnement ein („Empfohlen“). Das Abonnement umfasst die empfohlenen Versionen der gewählten Software.

Wenn Sie nicht die empfohlene Version abonnieren möchten, befolgen Sie die Konfigurationsanweisungen unter *Abonnieren von Sicherheitssoftware* (Seite 80).

Wenn Sie den Assistenten nach der Installation von Enterprise Console nicht ausgeführt haben, finden Sie im Abschnitt *Ausführen des Download-Assistenten für Sicherheitssoftware* (Seite 82) nähere Informationen.

6.2.2 Update-Arten

Jede Hauptversion einer Softwarelösung (z.B. Sophos Endpoint Security and Control 9) für die jeweiligen Betriebssysteme (z.B. Windows 2000 und höher) umfasst mehrere Versionen. Durch Festlegen einer Update-Art können Sie die Softwareversion auswählen, die von Sophos heruntergeladen werden und auf den Endpoints installiert werden soll. Es stehen drei Software-Versionen kategorisierter Updates und drei Software-Versionen fester Updates zur Auswahl.

Kategorisierte Updates

Folgende Kategorien werden angeboten:

Kategorie	Beschreibung
Empfohlen	Die von Sophos für angemessen erachtete Version zum Bezug der aktuellen Produktversion. In der Regel empfiehlt sich die Installation der neuesten Version der Endpoint-Software auf Computern.
Vorherig	Die vorab empfohlene Version.
Alt	Die älteste Softwareversion, für die Sophos Updates anbietet.

Hinweis: Möglicherweise werden künftig weitere Kategorien folgen.

Wenn Sie mit dem **Download-Assistent für Sicherheitssoftware** ein Abonnement einrichten, werden jeweils die empfohlenen Softwareversionen für Updates ausgewählt.

Wenn Sie eine Version mit einer bestimmten Bezeichnung abonniert haben, wird die heruntergeladene Version in der Regel monatlich geändert.

Feste Updates

Feste Versionen werden mit neuen Threat-Erkennungsdaten, jedoch nicht mit den monatlichen Software-Updates upgedatet.

Wenn Sie neue Versionen vor der Installation im Hauptnetzwerk testen möchten, empfiehlt sich, bis zum Abschluss der Tests feste Updates im Hauptnetzwerk einzusetzen.

In der Regel sind drei Versionen fester Updates für jedes Betriebssystem erhältlich (die Updates der vergangenen drei Monate). Ein festes Update kann etwa wie folgt aussehen: Sophos Endpoint Security and Control für Windows 2000 und höher, Version 9.4.3.

Feste Updates werden von Sophos heruntergeladen, bis sie eingestellt werden. Bei Einstellung eines festen Updates wird neben allen **Update Managern**, die diese Version abonnieren, ein Alert angezeigt. Wenn E-Mail-Benachrichtigungen aktiviert sind, wird der Administrator zudem per E-Mail darüber informiert.

Standardmäßig nimmt Enterprise Console bei Einstellung eines festen Updates das älteste verfügbare feste Update in das Abonnement auf.

Hinweis: Diese können Sie durch Deaktivieren des Kontrollkästchens **Nicht mehr unterstützte Abonnements einer bestimmten Version automatisch updaten** im Abonnement ändern. Wenn Sie nicht unterstützte Software ausführen, ist Ihr Computer vor neuen Threats nicht geschützt. Es empfiehlt sich daher, umgehend auf eine unterstützte Version upzudaten.

6.2.3 Abonnieren von Sicherheitssoftware

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Updates** verfügen, um Änderungen an einem Software-Abonnement vornehmen zu können.
- Wenn ein Abonnement einer Update-Richtlinie angehört, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befindet, können Sie es nicht ändern.

Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 17) entnehmen.

So können Sie Sicherheitssoftware abonnieren:

1. Klicken Sie im Menü **Ansicht** auf **Update Manager**.
2. Doppelklicken Sie im Fenster **Software-Abonnements** auf das zu ändernde Abonnement oder klicken Sie zum Erstellen eines neuen Abonnements auf **Hinzufügen**.

   Das Dialogfenster **Software-Abonnements** wird angezeigt.

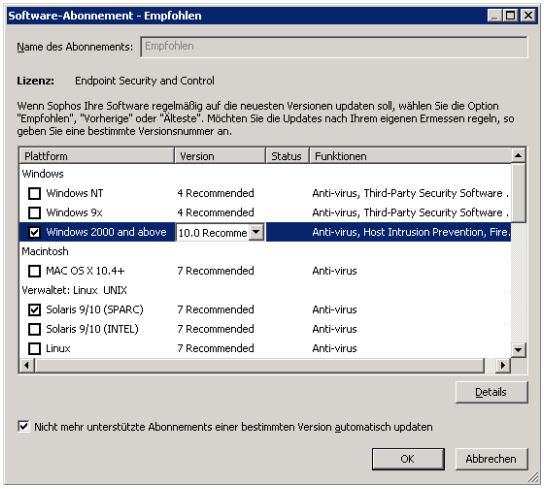
   Wenn Sie eine Kopie eines vorhandenen Abonnements anlegen möchten, rechtsklicken Sie auf das Abonnement und wählen Sie **Abonnement duplizieren**. Geben Sie dem Abonnement einen neuen Namen und doppelklicken Sie darauf. Das Dialogfeld **Software-Abonnement** wird geöffnet.
3. Im Dialogfeld **Software-Abonnements** können Sie auf Wunsch den Namen des Abonnements ändern.
4. Wählen Sie die Betriebssysteme aus, für die Sie Software herunterladen möchten.

   Wichtig: Wenn Sie Sophos Anti-Virus für NetWare herunterladen möchten, lesen Sie bitte auf der Sophos Website den Support-Artikel 59192 (*http://www.sophos.de/support/knowledgebase/article/59192.html*).

5. Für jede ausgewählte Plattform gilt: Klicken Sie neben der Plattform in das Feld **Version** und klicken Sie nochmal. Wählen Sie in der Dropdown-Liste die gewünschte Version aus, die Sie herunterladen möchten.

   In der Regel bietet sich die Option *empfohlene* Version an, da so sichergestellt wird, dass Software automatisch auf dem neuesten Stand gehalten wird. Im Abschnitt *Update-Arten* (Seite 79) können Sie sich über weitere Update-Arten informieren.

   Wichtig: Wenn Sie eine „feste Version“ (z.B. 10.1.2) ausgewählt haben, empfiehlt es sich, die Option **Nicht mehr unterstützte Abonnements einer bestimmten Version automatisch updaten** nicht zu deaktivieren. Wenn Sie nicht unterstützte Software nutzen, sind Ihre Computer vor neuen Threats nicht sicher.



Wenn Sie Sophos Sicherheitssoftware abonniert haben, können Sie Abonnement-Alerts einrichten. Nähere Informationen zu Abonnement-E-Mail-Alerts können Sie dem Abschnitt *Einrichten von Softwareabonnement-Alerts* (Seite 201) entnehmen.

Konfigurieren Sie den Update Manager nach dem Erstellen des neuen Software-Abonnements, damit er wie unter *Anzeigen oder Ändern der Update Manager-Konfiguration* (Seite 69) erläutert verwaltet wird.

6.2.4 Abonnieren von Verschlüsselungssoftware

Hinweis: Es empfiehlt sich, ein neues Abonnement für Verschlüsselung zu erstellen. Updates der Verschlüsselungssoftware erfolgen über den Assistenten zum Schutz von Computern. Nähere Informationen finden Sie unter *Automatische Installation von Verschlüsselungssoftware* (Seite 53).

So können Sie Verschlüsselungssoftware abonnieren:

1. Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Update Manager**.
2. Klicken Sie oben im Bereich **Software-Abonnements** auf **Hinzufügen**, um ein neues Abonnement einzurichten. Geben Sie im Fenster **Software-Abonnement** in das Feld **Name des Abonnements** den Namen ein. Klicken Sie unter **Verschlüsselungsprodukte** neben **Windows XP und höher** in das Feld **Version** und wählen Sie **5.61 empfohlen** aus. Klicken Sie auf **OK**.

3. Zum Hinzufügen des Abonnements zu den **Update Managern** rechtsklicken Sie im Feld **Update Manager** auf den Update Manager und wählen Sie **Konfiguration öffnen/ändern**. Wählen Sie im Dialogfeld **Update Manager konfigurieren** auf der Registerkarte **Abonnements** das Abonnement in der Liste **verfügbarer Abonnements** aus und fügen Sie es mit Hilfe der Schaltfläche „>“ in die Liste **Abonniert für**. Klicken Sie auf **OK**.

Die Verschlüsselungssoftware wird in die Standardfreigabe heruntergeladen: \\<Servername>\SophosUpdate\CIDs\<Abonnement>\ENCRYPTION.

Hinweis: Sie können die Verschlüsselungssoftware nicht durch Übertragen von Update-Richtlinien auf Computergruppen installieren. Installation und Updates der Verschlüsselungssoftware erfolgen über den Assistenten zum Schutz von Computern. Nähere Informationen finden Sie unter *Automatische Installation von Verschlüsselungssoftware* (Seite 53).

6.2.5 Ausführen des Download-Assistenten für Sicherheitssoftware

Bei rollenbasierter Verwaltung müssen Sie zum Ausführen des **Download-Assistenten für Sicherheitssoftware** über die Berechtigung **Richtlinieneinstellung – Updates** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wenn Sie den **Download-Assistenten für Sicherheitssoftware** nach der Installation von Enterprise Console nicht ausgeführt haben, verfahren Sie wie folgt:

- Klicken Sie im Menü **Maßnahmen** auf **Ausführen des Download-Assistenten für Sicherheitssoftware**.

  Der **Download-Assistent für Sicherheitssoftware** leitet Sie durch die Softwareauswahl und den Download.

6.2.6 Update-Richtlinien, die Software-Abonnements nutzen

So können Sie feststellen, welche Update-Richtlinien ein Software-Abonnement nutzen:

- Wählen Sie das Software-Abonnement aus, rechtsklicken Sie darauf und klicken Sie auf **Abonnement-Statistik anzeigen**.

  Im Dialogfeld **Software-Abonnement-Nutzung** werden die Update-Richtlinien aufgelistet, die das Abonnement nutzen.

6.3 Konfigurieren der Update-Richtlinie

6.3.1 Update-Richtlinie

Update-Richtlinien halten die Sicherheitssoftware auf Ihren Computern auf dem neuesten Stand. Enterprise Console sucht nach Updates und aktualisiert Computer in festgelegten Zeitabständen bei Bedarf.

Die Standard-Update-Richtlinie ermöglicht Installation und Updates der Software, die im „empfohlenen“ Abonnement angegeben sind.

Anweisungen zum Ändern der Standard-Update-Richtlinie oder Erstellen einer neuen Richtlinie finden Sie in den folgenden Abschnitten.

- *Auswahl eines Abonnements* (Seite 83)
- *Update-Server-Standorte* (Seite 84)
- *Update-Zeitpläne* (Seite 88)
- *Ändern der Erstinstallationsquelle* (Seite 89)
- *Update-Protokoll* (Seite 90)

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 17) entnehmen.

6.3.2 Auswahl eines Abonnements

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Durch Software-Abonnements wird festgelegt, welche Endpoint-Softwareversionen für die jeweiligen Systeme von Sophos heruntergeladen werden. Das Standard-Abonnement umfasst die aktuelle Software für Windows 2000 und höher.

So können Sie ein Abonnement auswählen:

1. Prüfen Sie, welche Update-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Update**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Update-Richtlinie** auf die Registerkarte **Abonnements** und wählen Sie ein Abonnement für Software, die Sie auf dem neuesten Stand halten möchten.

6.3.3 Konfigurieren der Update-Server-Standorte

6.3.3.1 Update-Server-Standorte

Die Standard-Update-Quelle ist eine einzelne primäre UNC-Freigabe, \\<ComputerName>\SophosUpdate. <ComputerName> ist dabei der Name des Computers mit dem Update Manager. Auf Wunsch können Sie auch eine alternative sekundäre Update-Quelle angeben und Standort-Roaming aktivieren. Wenn Endpoints keine Verbindung zur primären Quelle herstellen können, versuchen sie, Updates von der sekundären Quelle (falls vorhanden) zu beziehen. Es empfiehlt sich, stets eine sekundäre Quelle anzugeben.

Bei dem primären und sekundären Update-Server-Verzeichnis handelt es sich um eine UNC-Freigabe oder HTTP-URL von einem verfügbaren Update Manager im Netzwerk. Für die sekundäre Update-Quelle kann auch angegeben werden, dass Updates per HTTP über das Internet direkt von Sophos bezogen werden.

Hinweis: Je nach Konfiguration stehen Update Managern mitunter mehrere Verteilungsfreigaben zur Verfügung.

6.3.3.2 Standort-Roaming

6.3.3.2.1 Laptop-Roaming

Unter Umständen roamen Mitarbeiter mit Laptops sehr viel, auch international. Bei aktiviertem Standort-Roaming (in der Update-Richtlinie für Roaming-Laptops) suchen Roaming-Laptops nach dem nächsten Update-Server und versuchen, von diesem Updates zu beziehen. Hierzu senden sie eine Anfrage an andere (feste) Endpoints im lokalen Netzwerk, mit dem sie verbunden sind, um Update-Zeit und Bandbreite einzusparen.

Roaming-Laptops beziehen Update-Server-Standorte und Zugangsdaten, indem sie eine Anfrage an feste Computer im gleichen lokalen Netzwerk beziehen. Wenn mehrere Standorte gefunden werden, sucht das Laptop nach dem nächsten und greift auf diesen zu. Wenn dies nicht möglich ist, greift das Laptop auf den in der Update-Richtlinie festgelegten primären (und anschließend den sekundären) Standort zu.

Hinweis: Wenn feste Computer Update-Standorte und Zugangsdaten an das Laptop senden, sind die Kennwörter bei der Übertragung und Speicherung verschleiert. Konten zum Lesen der Update-Server-Standorte sollten nur mit Lesezugriff ausgestattet werden. Mehr dazu erfahren Sie unter *Festlegen des Download-Verzeichnisses* (Seite 72).

Nähere Informationen zur Funktionsweise von Standort-Roaming finden Sie unter *Funktionsweise von Standort-Roaming* (Seite 85).

Standort-Roaming ist nur in folgenden Fällen möglich:

- Roaming-Endpoints und feste Endpoints greifen auf die gleiche Enterprise Console zu.
- Das Software-Abonnement von festen Endpoints und Roaming-Laptops ist identisch.
- Eine primäre Update-Quelle wurde in der Update-Richtlinie der roamanden Laptops festgelegt.
- Enterprise Console ist Version 4.7 oder höher und Endpoint Security and Control ist Version 9.7 oder höher auf festen und Roaming-Endpoints.

- In Firewalls von anderen Anbietern sind Update-Standort-Anfragen und -Antworten zugelassen. Der Standortport lautet „51235“, ist jedoch konfigurierbar. Details finden Sie hier: *http://www.sophos.de/support/knowledgebase/article/110371.html*.

Sie können Standort-Roaming bei der Angabe von Update-Quellen aktivieren. Sie sollten Standort-Roaming nur auf Systemen aktivieren, die häufig im Wechsel im Unternehmen und extern verwendet werden. Nähere Informationen zum Aktivieren von Standort-Roaming können Sie dem Abschnitt *Ändern der Zugangsdaten zum Primärserver* (Seite 86) entnehmen.

Häufig gestellte Fragen zu Standort-Roaming werden im Sophos Support-Artikel 112830 (*http://www.sophos.de/support/knowledgebase/article/112830.html*) beantwortet.

6.3.3.2.2 Funktionsweise von Standort-Roaming

Standort-Roaming ist eine intelligente Update-Methode für roamende Laptops. Updates werden dabei vom geeignetsten Update-Verzeichnis bezogen. Die Update-Funktion ist also nicht auf die in der Update-Richtlinie des Laptops angegebene primäre oder sekundäre Update-Quelle beschränkt.

Bei aktiviertem Standort-Roaming geschieht Folgendes:

1. Wenn ein Laptop den Standort ändert, stellt Sophos AutoUpdate, eine auf dem Laptop installierte Komponente von Endpoint Security and Control, eine Änderung der MAC-Adresse des Standard-Gateways auf dem verbundenen Netzwerk seit dem letzten Update fest. Es folgt eine ICMP-Kommunikation über das lokale Subnetz an benachbarte AutoUpdate-Installationen. Dies erfolgt standardmäßig über Port 51235.
2. Die benachbarten AutoUpdate-Installationen senden eine Antwort über den gleichen Port unter Bezugnahme auf ihre Update-Richtlinien. Die Antwort umfasst nur die primäre Update-Quelle.

   Ab Endpoint Security and Control 9.7 befindet sich die Software stets im Listening-Modus, egal ob Standort-Roaming aktiviert ist oder nicht.

   Sensible Daten werden verschleiert und umfassen einen Hash zur Überprüfung der Integrität.

   Antworten erfolgen zu willkürlichen Zeiten, um Überlastungen zu vermeiden. Bei den Antworten handelt es sich auch um ICMP-Kommunikationen. Alle Systeme, die mit den gleichen Details geantwortet haben, erhalten die Meldung und wissen, dass sie nicht antworten sollen.
3. AutoUpdate ermittelt das beste Verzeichnis aus den Antworten und prüft, ob der Sender von der gleichen Enterprise Console verwaltet wird und ob die Abonnement-Kennung der Kennung von AutoUpdate des Laptops entspricht.

   Das beste Update-Verzeichnis richtet sich nach der Anzahl der Hops, die zum Zugriff auf das Verzeichnis erforderlich sind.
4. Es wird ein Update-Versuch gestartet. Ist das Update erfolgreich, wird das Verzeichnis gecacht.

   Maximal vier verfügbare Update-Verzeichnisse mit der gleichen Abonnement-Kennung und der geringsten Hop-Anzahl werden auf dem Laptop gespeichert (in der Datei iustatus.xml hier: C:\Programme\Sophos\AutoUpdate\data\status\iustatus.xml).

   Die Update-Verzeichnisse werden bei jedem Update von AutoUpdate abgerufen.

Hinweis: Wenn Sie wieder zur primären oder sekundären Update-Quelle in der Update-Richtlinie wechseln müssen (weil sie etwa die benutzerdefinierten Einstellungen des in der Update-Richtlinie angegebenen Verzeichnisses implementieren möchten), müssen Sie Standort-Roaming deaktivieren.

6.3.3.2.3 Aktivieren von Standort-Roaming

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie sollten Standort-Roaming nur auf Systemen aktivieren, die häufig im Wechsel im Unternehmen und extern verwendet werden.

So aktivieren Sie Standort-Roaming:

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Update**. Doppelklicken Sie dann auf die Update-Richtlinie, die Sie ändern möchten.
2. Klicken Sie im Dialogfeld **Update-Richtlinie** auf die Registerkarte **Primärserver** und aktivieren Sie das Kontrollkästchen **Standort-Roaming zulassen**.
3. Wählen Sie im Feld **Gruppen** eine Gruppe aus, die die soeben geänderte Update-Richtlinie verwendet. Rechtsklicken Sie auf die Auswahl und wählen Sie **Konformität mit** > **Gruppen-Update-Richtlinie**.

   Wiederholen Sie diesen Schritt für alle Gruppen in der Richtlinie.

Hinweis: Wenn Sie zu einem späteren Zeitpunkt wieder zu der primären oder sekundären Update-Quelle aus der Update-Richtlinie wechseln müssen, deaktivieren Sie das Standort-Roaming.

6.3.3.3 Ändern der Zugangsdaten zum Primärserver

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So ändern Sie die Zugangsdaten des Primärservers:

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Update**. Doppelklicken Sie dann auf die Update-Richtlinie, die Sie ändern möchten.

2. Geben Sie im Dialogfeld **Update-Richtlinie** auf der Registerkarte **Primärserver** die neuen Zugangsdaten zum Zugang für den Server ein. Sie können bei Bedarf auch andere Angaben ändern.

   Hinweis: Wenn es sich bei der primären Update-Quelle um einen Ordner auf Ihrer Website handelt und Sie die Internetinformationsdienste (IIS) mit anonymer Authentifizierung verwenden, müssen Sie Ihre Zugangsdaten trotzdem am **Primärserver** angeben. Verwenden Sie die Zugangsdaten für die UNC-Freigabe der Erstinsallationsquelle, auch wenn Sie sie nicht für den Zugriff auf den Webserver benötigen. Wenn Sie die Felder **Benutzername** und **Kennwort** auf der Registerkarte **Prinärserver** nicht ausfüllen, können Sie die Endpoints nicht über die Konsole schützen.

3. Wählen Sie im Feld **Gruppen** eine Gruppe aus, die die soeben geänderte Update-Richtlinie verwendet. Rechtsklicken Sie auf die Auswahl und wählen Sie **Konformität mit** > **Gruppen-Update-Richtlinie**.

   Wiederholen Sie diesen Schritt für alle Gruppen in der Richtlinie.

6.3.3.4 Festlegen des sekundären Update-Server-Standorts

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So legen Sie den sekundären Update-Server-Standort fest:

1. Prüfen Sie, welche Update-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Feld **Richtlinien** auf **Updates** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Update-Richtlinie** auf die Registerkarte **Sekundärserver** und aktivieren Sie das Kontrollkästchen **Sekundärserver festlegen**.
4. Das Feld **Adresse** bietet folgende Optionen:

   - Eingabe der HTTP-URL bzw. des UNC-Netzwerkpfads der Update-Server-Freigabe.
   - Auswahl von **Sophos**.

   Wichtig: Wenn Sie eine HTTP-URL oder eine Freigabe auswählen, die nicht von einem verwalteten Update Manager verwaltet wird, kann Enterprise Console nicht überprüfen, ob das angegebene Software-Abonnement verfügbar ist. Stellen Sie sicher, dass die Freigabe das angegebene Abonnement enthält, da Computer andernfalls keine Updates beziehen.

5. Wenn die Richtlinie Mac-Endpoints umfasst und Sie im **Adressfeld** unter **Wählen Sie ein File Sharing-Protokoll für Mac OS X** einen UNC-Pfad angegeben haben, wählen Sie ein Protokoll für den Zugriff der Macs auf die Update-Freigabe aus.

6. Geben Sie bei Bedarf den **Benutzernamen** für den Zugriff auf den Server ein. Geben Sie dann das Kennwort ein und bestätigen Sie das Kennwort. Bei Sophos HTTP handelt es sich um die Zugangsdaten des Abonnements.

   Das Konto muss Lesezugriff (Navigationsszugriff) auf die Freigabe besitzen, die Sie oben in das Adressfeld eingegeben haben.

   Hinweis: Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein. Nähere Informationen zum Überprüfen eines Windows-Benutzerkontos finden Sie im Sophos Support-Artikel 11637 (*http://www.sophos.de/support/knowledgebase/article/11637.html*).

7. Klicken Sie zum Verringern der Bandbreite auf **Erweitert**. Aktivieren Sie im Dialogfeld **Erweiterte Einstellungen** die Option **Bandbreite verringern** und geben Sie mit Hilfe des Schiebereglers die Bandbreite in KBit/s an.
8. Wenn Sie über einen Proxyserver auf die Update-Quelle zugreifen, klicken Sie auf **Proxyserver-Details**. Aktivieren Sie im Dialogfeld **Proxy-Details** die Option **Internetverbindung über Proxyserver herstellen** und geben Sie dann **Adresse** und **Portzahl** des Proxyservers ein. Geben Sie die **Zugangsdaten** des Proxyservers ein. Falls der Benutzername auch eine Domäne erfordert, geben Sie ihn im Format Domäne\Benutzername ein.

   Hinweis: Bei einigen Internet Service Providern werden HTTP-Anfragen an einen Proxyserver gesendet.

9. Klicken Sie auf **OK**, um das Fenster **Updating-Richtlinie** zu schließen.
10. Rechtsklicken Sie im Fenster **Gruppen** auf eine Gruppe, die die soeben geänderte Update-Richtlinie nutzt und klicken Sie anschließend auf **Konformität mit** > **Update-Gruppenrichtlinie** .

    Wiederholen Sie diesen Schritt für alle Gruppen in der Richtlinie.

6.3.4 Update-Zeitpläne

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Standardmäßig suchen Endpoints alle 5 Minuten nach Updates in den Netzwerkfreigaben.

Hinweis: Wenn Updates direkt von Sophos heruntergeladen werden, werden die Update-Intervalleinstellungen nicht übernommen. Computer mit Sophos PureMessage können alle 15 Minuten nach Updates suchen. Computer ohne Sophos PureMessage werden alle 60 Minuten aktualisiert.

So können Sie das Update-Intervall festlegen:

1. Prüfen Sie, welche Update-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Update**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Rufen Sie im Dialogfeld **Update-Richtlinie** die Registerkarte **Zeitplan** auf und stellen Sie sicher, dass das Kontrollkästchen **Sophos Updates automatisch herunterladen** aktiviert ist. Geben Sie ein Intervall für Software-Updates (in Minuten) ein.
4. Wenn Sie Updates über eine Einwahlverbindung durchführen, wählen Sie **Bei Internetverbindung auf Updates prüfen**.

   Die Computer versuchen dann, bei jeder Verbindungsherstellung ein Update durchzuführen.

6.3.5 Ändern der Erstinstallationsquelle

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Standardmäßig wird Sicherheitssoftware auf Computern installiert und dann über die auf der Registerkarte **Primärserver** angegebenen Quelle aktualisiert. Sie können eine andere Quelle für die Erstinstallation angeben.

Hinweis:

Diese Einstellung ist nur für Windows 2000 und höher relevant.

Wenn Ihr Primärserver eine HTTP- (Internet)-Adresse ist und Sie die Installation auf den Computern von der Konsole aus durchführen möchten, müssen Sie eine Quelle für die Erstinstallation angeben.

So können Sie die Quelle für die Erstinstallation ändern:

1. Prüfen Sie, welche Update-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Update**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Deaktivieren Sie im Dialogfeld **Update-Richtlinie** auf der Registerkarte **Erstinstallationsquelle** das Kontrollkästchen **Adresse des Primärservers übernehmen**. Geben Sie dann die Adresse der gewünschten Quelle ein.

6.3.6 Update-Protokoll

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Update-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Updates** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Standardmäßig wird die Update-Aktivität von Computern protokolliert. Das Protokoll darf standardmäßig maximal 1 MB umfassen. Die Voreinstellung für den Protokollgrad lautet „normal“.

So können Sie die Protokolleinstellungen ändern:

1. Prüfen Sie, welche Update-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Update**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Stellen Sie sicher, dass im Dialogfeld **Update-Richtlinie** auf der Registerkarte **Protokollierung** die Option **Sophos AutoUpdates protokollieren** aktiviert ist. Geben Sie in das Feld **Max. Protokollgröße** die gewünschte Größe in MB ein.
4. Wählen Sie im Feld **Protokollgrad** die Option **Normal** oder **Ausführlich** aus.

   In ausführlichen Protokollen werden mehr Aktivitäten protokolliert als gewöhnlich, was sich auch auf die Protokollgröße auswirkt. Verwenden Sie diese Einstellung nur, wenn Sie das ausführliche Protokoll zur Problembehebung benötigen.

6.4 Überwachen des Update Managers

6.4.1 Übersicht über Update Manager

Überprüfen des Update Manager-Status auf dem Dashboard

Der Status des Update Managers wird im Bereich **Updates** auf dem **Dashboard** angezeigt. Hier können Sie sehen, wann das letzte Update von Sophos heruntergeladen wurde. Wenn die seit dem letzten Update verstrichene Zeit über dem Warnschwellenwert bzw. kritischen Schwellenwert liegt, wird ein Warnhinweis angezeigt.

Hinweis: Im Abschnitt **Updates** des Dashboards wird kein Alert oder Fehler angezeigt, wenn ein Update Manager vorübergehend keine Updates beziehen kann. Es werden lediglich dann Alerts oder Fehler angezeigt, wenn die seit dem letzten Update verstrichene Zeit über dem in *Konfigurieren des Dashboards* (Seite 56) festgelegten Warnschwellenwert bzw. kritischen Schwellenwert liegt.

Überprüfen von Alerts und Fehlern der Update Manager

Alerts und Fehlern der Update Manager werden in der Ansicht **Update Manager** in der Spalte **Alerts** bzw. **Fehler** angezeigt.

Wenn Sie eine bestimmte Softwareversion abonniert haben, wird ein Alert angezeigt, wenn die Version demnächst eingestellt wird oder eingestellt wurde. Auch bei Änderungen der Produktlizenz wird ein Alert angezeigt.

So können Sie sich Alerts und Fehlern der Update Manager anzeigen lassen:

1. Wenn Sie sich in der Ansicht **Endpoints** befinden, klicken Sie in der Symbolleiste auf das **Update Manager**-Symbol. Die Ansicht **Update Manager** wird angezeigt.
2. Suchen Sie in der Update Manager-Liste in den Spalten **Alerts** und **Fehler** nach möglichen Problemen.
3. Wenn neben einem Update Manager ein Alert oder Fehler angezeigt wird, rechtsklicken Sie auf den Update Manager und klicken Sie auf die Option **Update Manager-Details**.

   Im Dialogfeld **Update Manager-Details** werden der Zeitpunkt der letzten Software- und Threaterkennungsdaten-Updates, der Status der vom Update Manager verwalteten Abonnements und der Status des Update Managers angezeigt.
4. Nähere Informationen zum Status eines Update Managers und zur Fehlersuche finden Sie in der Spalte **Beschreibung**.

Wenn Sie Ihre Abonnements aufrufen oder ändern möchten, weil beispielsweise ein Produkt demnächst eingestellt wird oder sich die Lizenz geändert hat, ziehen Sie den Abschnitt *Abonnieren von Sicherheitssoftware* (Seite 80) zu Rate.

Wenn nach einer Lizenzänderung neue Funktionen verfügbar sind, müssen Sie unter Umständen neue Richtlinien konfigurieren. Die Konfiguration der neuen Richtlinien wird im Abschnitt *Konfigurieren von Richtlinien* erläutert.

Abonnieren von E-Mail-Benachrichtigungen

Sie können Ihre gewählten Empfänger per E-Mail über (baldige) Produkteinstellungen oder Änderungen des Funktionsumfangs von Sophos Software im Zuge einer Lizenzänderung benachrichtigen lassen. Weitere Informationen finden Sie unter *Einrichten von Softwareabonnement-Alerts* (Seite 201).

6.4.2 Löschen von Update Manager-Alerts aus der Konsole

Bei rollenbasierter Administration gilt als Voraussetzung für das Löschen von Alerts die Berechtigung **Korrektur – Bereinigung**. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So löschen Sie Update Manager-Alerts aus der Konsole:

1. Markieren Sie in der Ansicht **Update Manager** die zu löschenden Alerts. Rechtsklicken Sie und wählen Sie **Alerts löschen**.

   Das Fenster **Update Manager-Alerts** wird angezeigt.

2. Um die Alerts zu löschen, wählen Sie die gewünschten Alerts aus und klicken Sie auf **Löschen**.

   Gelöschte Alerts werden nicht mehr in der Konsole angezeigt.

6.5 Updaten nicht aktueller Computer

Bei rollenbasierter Verwaltung müssen Sie zum Updaten von Computern über die Berechtigung **Korrektur – Updates und Scans** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Nach dem Einrichten der Update-Richtlinien und der Übernahme der Richtlinien auf Netzwerkcomputern, werden die Computer automatisch auf dem neuesten Stand gehalten. Sofern kein Problem mit der Update-Funktion vorliegt, müssen Sie Computer nicht manuell updaten.

Wenn in der Computerliste in der Ansicht **Endpoints** ein Uhrsymbol neben einem Computer in der Spalte **Auf dem neuesten Stand** auf der Registerkarte **Status** angezeigt wird, befindet sich die Sicherheitssoftware des Computers nicht mehr auf dem aktuellen Stand. Aus dem Text geht hervor, seit wann sich der Computer nicht mehr auf dem neuesten Stand befindet.

Ein Computer kann aus einem von zwei Gründen nicht aktuell sein:

- Der Computer hat kein Update vom Server erhalten.
- Auf dem Server ist nicht die neueste Sophos Software verfügbar.

So können Sie das Problem bestimmen und die Computer updaten:

1. Wählen Sie in der Ansicht **Endpoints** die Gruppe mit den Computern aus, die sich nicht auf dem neuesten Stand befinden.
2. Klicken Sie in der Registerkarte **Status** auf die Spalte **Auf dem neuesten Stand**, um die Computer nach Aktualität zu sortieren.
3. Klicken Sie auf die Registerkarte **Update-Details** und sehen Sie in der Spalte **Primärserver** nach.

   Dort wird das Verzeichnis angezeigt, von dem aus die Computer jeweils ihre Updates beziehen.

4. Sehen Sie sich jetzt die Computer an, die sich von einem bestimmten Verzeichnis aus aktualisieren.

   - *Wenn einige nicht aktuell sind, andere aber doch*, besteht das Problem auf einzelnen Computern. Rechtsklicken Sie darauf und klicken Sie auf die Option **Computer jetzt updaten**.
   - *Wenn alle Computer nicht aktuell sind*, könnte das Problem am Verzeichnis liegen. Klicken Sie im Menü **Ansicht** auf **Update Manager**. Rechtsklicken Sie auf den Update Manager, der das Verzeichnis auf dem neuesten Stand hält, von dem Sie vermuten, dass es nicht aktuell ist, und wählen Sie **Jetzt updaten**. Klicken Sie im Menü **Ansicht** auf **Endpoints**. Wählen Sie die Computer aus, die nicht mehr aktuell sind, rechtsklicken Sie darauf und klicken Sie auf **Computer jetzt updaten**.

Wenn Sie mehrere Update Manager besitzen, können Sie im Update-Hierarchie-Report nachsehen, welche Freigaben von den einzelnen Update Managern auf dem neuesten Stand gehalten werden. Zum Aufrufen des Update-Hierarchie-Reports klicken Sie im Menü **Extras** auf **Report-Verwaltung**. Wählen Sie im Dialogfeld **Update-Richtlinie** die Option **Report Manager** und klicken Sie auf **Ausführen**. Sehen Sie sich den Report-Abschnitt „Von Update-Managern verwaltete Freigaben“ an.

7 Konfigurieren von Richtlinien

7.1 Konfigurieren der Antivirus- und HIPS-Richtlinie

7.1.1 Die Antivirus- und HIPS-Richtlinie

Anti-Virus- und HIPS-Richtlinien dienen der Erkennung und Beseitigung von Viren, Trojanern, Würmern, Spyware sowie Adware und anderen potenziell unerwünschten Anwendungen. Zudem können Sie mit der Richtlinie nach verdächtigem Verhalten, verdächtigen Dateien und Rootkits suchen. Sie können den Computergruppen jeweils unterschiedliche Einstellungen zuweisen.

Standardmäßig bietet Sophos Endpoint Security and Control folgende Optionen:

- Automatische Erkennung bekannter und unbekannter Viren, Trojaner, Würmer und Spyware, sobald ein Anwender versucht, auf Dateien zuzugreifen, in denen sie enthalten sind.
- Verhaltensanalyse der Programme, die auf dem System laufen.
- Automatische Bereinigung von Computern bei Erkennen von Viren oder sonstigen Threats.

Hinweis: Sie können die Einstellungen der automatischen Bereinigung anhand der Anweisungen im Abschnitt *Einrichten der automatischen Bereinigung für On-Access-Scans* (Seite 65) ändern.

Sie können außerdem Sophos Endpoint Security and Control dazu konfigurieren, Folgendes auszuführen:

- *Scannen auf verdächtige Dateien im Rahmen von On-Access-Scans* (Seite 102)
- *Scannen auf Adware und PUA* (Seite 96)
- *Scannen von Computern zu bestimmten Zeiten* (Seite 108)

Hinweis: Enterprise Console kann auf UNIX-Computern keine On-Access-Scans durchführen. Verwenden Sie eine andere Scan-Option oder ziehen Sie das *Benutzerhandbuch zu Sophos Anti-Virus für UNIX* zu Rate.

7.1.2 Scannen auf Viren, Trojaner, Würmer und Spyware

Standardmäßig erkennt Sophos Endpoint Security and Control bekannte und unbekannte Viren, Trojaner, Würmer und Spyware automatisch, wenn ein Benutzer versucht, auf Dateien zuzugreifen, in denen sie enthalten sind.

7.1.3 Sophos Live-Schutz

7.1.3.1 Allgemeine Informationen

Dank Sophos Live-Schutz lässt sich über ein "In-the-Cloud"-Verfahren sofort feststellen, ob eine Datei eine Bedrohung darstellt. Bei Bedarf werden umgehend die in der Schutzkonfiguration der Antivirus- und HIPS-Richtlinie festgelegten Maßnahmen ergriffen.

Die Malware-Erkennung wird durch den Live-Schutz erheblich verbessert, und es kommt nicht zu unerwünschten Erkennungen. Das Verfahren basiert auf einem Sofortabgleich mit den aktuellen Malwaredateien. Wenn neue Malware erkannt wird, kann Sophos binnen Sekunden Updates bereitstellen.

Folgende Optionen müssen zur Nutzung des Live-Schutzes aktiviert sein:

- **Live-Schutz aktivieren**

  Wenn eine Datei von einem Antiviren-Scan auf einem Endpoint als verdächtig eingestuft wurde, anhand der Threatkennungsdateien (IDEs) auf dem Computer jedoch nicht festgestellt kann, ob die Datei virenfrei ist, werden bestimmte Daten (z.B. die Prüfsumme der Datei) zur weiteren Analyse an Sophos übermittelt. Bei der "In-the-Cloud"-Prüfung wird durch Abgleich mit der Datenbank der SophosLabs festgestellt, ob es sich um eine verdächtige Datei handelt. Die Datei wird als virenfrei oder von Malware betroffen eingestuft. Das Ergebnis der Prüfung wird an den Computer übertragen, und der Status der Datei wird automatisch aktualisiert.

- **Dateisamples automatisch an Sophos senden**

  Wenn die Datei als potenzielle Malware eingestuft wird, anhand der Eigenschaften der Datei jedoch keine eindeutige Klassifizierung möglich ist, kann Sophos über den Live-Schutz ein Dateisample anfordern. Wenn diese Option aktiviert ist und Sophos noch kein Dateisample vorliegt, wird die Datei automatisch an Sophos übermittelt.

  Dateisamples helfen Sophos bei der Optimierung der Malware-Erkennung und minimieren falsche Erkennungen (sog. „False Positives“).

  Hinweis: Samples dürfen maximal 10 MB groß sein. Das Zeitlimit für den Sample-Upload beträgt 30 Sekunden. Es wird davon abgeraten, Samples über eine langsamen Internetverbindung zu übertragen (weniger als 56 kbit/s).

Wichtig: Sie müssen sicherstellen, dass die Sophos-Domäne, an die die Dateidaten gesendet werden, in Ihrer Web-Filter-Lösung zu den vertrauenswürdigen Seiten hinzugefügt wurde. Weitere Informationen entnehmen Sie bitte dem Support-Artikel 62637 (*http://www.sophos.de/support/knowledgebase/article/62637.html*).

Wenn Sie eine Web-Filter-Lösung von Sophos einsetzen (z.B. WS1000 Web Appliance), müssen Sie nicht tätig werden, da Sophos-Domänen zu den vertrauenswürdigen Seiten zählen.

7.1.3.2 Aktivieren/Deaktivieren von Sophos Live-Schutz

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.

- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Standardmäßig übermittelt Endpoint Security and Control Dateidaten an Sophos (z.B. Prüfsummen), jedoch keine Dateisamples. Aktivieren Sie beide Optionen, um Sophos Live-Schutz in vollem Umfang ausnutzen zu können.

So aktivieren/deaktivieren Sie die Optionen von Sophos Live-Schutz:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** auf die Schaltfläche **Sophos Live-Schutz**.
4. Verfahren Sie im Dialogfeld **Sophos Live-Schutz** wie folgt:

   - Wenn Sie das Senden von Dateidaten an Sophos ein- bzw. ausschalten möchten, aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Live-Schutz aktivieren**.
   - Wenn Sie das Senden von Dateisamples an Sophos ein- bzw. ausschalten möchten, aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Dateisamples automatisch an Sophos senden**.

   Hinweis: Wenn ein Datei-Sample an Sophos zum Online-Scan gesendet wird, werden die Dateidaten immer mitgesendet.

7.1.4 Adware und PUA

7.1.4.1 Scannen auf Adware und PUA

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Hinweis: Die Option beschränkt sich auf Sophos Endpoint Security and Control für Windows 2000 und aufwärts.

Es empfiehlt sich, die Suche nach potenziell unerwünschten Anwendungen über einen geplanten Scan zu starten. Auf diese Weise können Sie gefahrlos Anwendungen bearbeiten, die *bereits*

auf Ihrem Computer aktiv sind. Sie können dann die On-Access-Erkennung aktivieren, um Ihre Computer in Zukunft zu schützen.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.

3. Klicken Sie im Fensterbereich **Geplante Scans** auf **Hinzufügen**, um einen neuen Scan zu erstellen, oder doppelklicken Sie auf einen Scan in der Liste, um ihn zu bearbeiten.
4. Im Dialogfeld **Einstellungen zu geplanten Scans** klicken Sie auf **Konfigurieren** (unten im Fenster).
5. Wählen Sie im Dialogfeld **Einstellungen zu Scans und Bereinigung ändern** auf der Registerkarte **Scans** im Bereich **Dateien scannen auf** das Kontrollkästchen **Adware und PUA**. Klicken Sie auf **OK**.

   Wenn der Scan ausgeführt wird, kann Sophos Endpoint Security and Control Adware oder potenziell unerwünschte Anwendungen melden.

6. Wenn Ihr Computer die Anwendungen starten soll, müssen Sie diese zulassen (mehr dazu erfahren Sie im Abschnitt *Zulassen von Adware und PUA* (Seite 97)). Andernfalls entfernen Sie die Anwendungen (mehr dazu erfahren Sie im Abschnitt *Sofortiges Bereinigen von Computern* (Seite 64)).
7. Wenn Sie die On-Access-Erkennung aktivieren möchten, öffnen Sie nochmals das Dialogfeld **Antivirus- und HIPS-Richtlinie**. Stellen Sie sicher, dass die Option **On-Access-Scans aktivieren** ausgewählt ist. Klicken Sie neben dem Kontrollkästchen auf die Schaltfläche **Konfigurieren**. Wählen Sie im Dialogfeld **On-Access-Scan-Einstellungen** unter **Scannen auf** die Option **Adware und PUA**.

   Hinweis: Einige Anwendungen „überwachen“ Dateien und versuchen, regelmäßig auf sie zuzugreifen. Wenn die On-Access-Scans aktiviert sind, werden alle Zugriffe erkannt und mehrere Alerts ausgegeben. Mehr dazu erfahren Sie unter *Hohe Alert-Anzahl aufgrund potenziell unerwünschter Anwendungen* (Seite 244).

7.1.4.2 Zulassen von Adware und PUA

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wenn Sie Sophos Endpoint Security and Control für die Erkennung von Adware und potenziell unerwünschten Anwendungen (PUA) konfiguriert haben, kann damit eventuell die Verwendung einer erwünschten Anwendung verhindert werden.

Verfahren Sie zum Zulassen erwünschter Anwendungen wie folgt:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** auf die Schaltfläche **Autorisierungen**.
4. Wählen Sie im Dialogfeld **Authorization Manager** auf der Registerkarte **Adware und PUA** in der Liste **Bekannte Adware/PUA** die gewünschte Anwendung. Klicken Sie auf **Hinzufügen**, um sie in die Liste **Zugel. Adware/PUA** aufzunehmen.
5. Wenn die zuzulassende Anwendung nicht angezeigt wird, klicken Sie auf **Neuer Eintrag**.

   Das Dialogfeld **Neue Adware/PUA** wird angezeigt.
6. Rufen Sie die Sicherheitsanalysen auf der Sophos Website *http://www.sophos.de/security/analyses/* auf. Suchen Sie auf der Registerkarte **Adware/PUA** die gewünschte Anwendung.
7. Geben Sie in Enterprise Console in das Dialogfeld **Neue Adware/PUA** den Namen der gewünschten Anwendung ein und klicken Sie auf **OK**.

   Die Anwendung wird in die Liste **Bekannte Adware/PUA** aufgenommen.
8. Wählen Sie die Anwendung aus und klicken Sie auf **Hinzufügen**, um sie in die Liste **Zugel. Adware/PUA** aufzunehmen.

Wenn Sie eine Anwendung aus der Liste entfernen möchten, wählen Sie die Anwendung und klicken Sie auf **Eintrag löschen**.

7.1.5 Web-Schutz

7.1.5.1 Der Web-Schutz

Der Web-Schutz bietet besseren Schutz vor Threats aus dem Internet. Die Komponente umfasst folgende Funktionen:

- Live-URL-Filterung, die den Zugriff auf Websites sperrt, auf denen bekanntermaßen Malware gehostet wird. Die Funktion basiert auf einem Online-Abgleich mit der Sophos Datenbank infizierter Websites.
- Inhalts-Scan-Funktion zum Scannen von aus dem Internet (oder Intranet) heruntergeladenen Daten und Dateien sowie proaktive Erkennung schädlicher Inhalte. Die Funktion dient dem Scannen von Inhalten, die an beliebigen Stellen gehostet werden, auch wenn sie nicht in der Datenbank infizierter Websites aufgeführt werden.

Der Web-Schutz wird von folgenden Browsern unterstützt: Internet Explorer, Firefox, Google Chrome, Safari und Opera. Inhalte, auf die über einen nicht unterstützten Browser zugegriffen wird, werden nicht gefiltert und folglich auch nicht gesperrt.

Wenn der Zugriff auf eine schädliche Website gesperrt wird, wird ein Ereignis protokolliert. Dies kann in der Web-Ereignisanzeige sowie den **Computerdetails** des Endpoints, auf dem

das Ereignis aufgetreten ist, abgerufen werden. Wenn Sie Web Control verwenden, werden Ereignisse von Web-Schutz und Web Control in der Web-Ereignisanzeige und den **Computerdetails** angezeigt. Nähere Informationen finden Sie unter *Anzeige von Web-Ereignissen* (Seite 220) und *Anzeige der aktuellen Web-Ereignisse auf einem Computer* (Seite 222).

Standardmäßig ist der Web-Schutz deaktiviert. Nähere Informationen zum Aktivieren/Deaktivieren des Web-Schutzes finden Sie unter *Aktivieren/Deaktivieren des Web-Schutzes* (Seite 99).

Hinweis: Web Control bietet Ihnen mehr Kontrolle über die Web-Nutzung der User. Wenn Sie etwa verhindern möchten, dass Mitarbeiter Websites aufrufen, deren Besuch rechtliche Folgen für Ihr Unternehmen nach sich ziehen kann, bietet sich Web Control an. Nähere Informationen finden Sie unter *Informationen zur Web Control-Richtlinie* (Seite 192).

7.1.5.2 Aktivieren/Deaktivieren des Web-Schutzes

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So aktivieren/deaktivieren Sie den Web-Schutz:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**.
3. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
4. Wählen Sie im Dialogfeld **Antiviren- und HIPS-Richtlinie** neben der Option **Zugriff auf schädliche Websites sperren Ein** oder **Aus**, um den Web-Schutz zu aktivieren oder deaktivieren. Diese Option ist standardmäßig aktiviert.

   Anweisungen zum Zulassen bestimmter Websites entnehmen Sie bitte dem Abschnitt *Zulassen von Websites* (Seite 99).
5. Wenn Sie das Scannen von aus dem Internet heruntergeladenen Daten und Dateien aktivieren/deaktivieren möchten, wählen Sie neben **Download-Scans** die Option **Ein**, **Wie On-Access** oder **Aus**.

   Die Standardoption lautet **Wie On-Access**. Das bedeutet, dass Download-Scans bei jeder Aktivierung/Deaktivierung von On-Access-Scans aktiviert/deaktiviert werden.

7.1.5.3 Zulassen von Websites

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Vorsicht: Wenn Sie Websites, die als schädlich eingestuft wurden, zulassen, sind Sie nicht vor Threats geschützt. Stellen Sie sicher, dass der Zugriff auf eine Website sicher ist, bevor Sie sie zulassen.

Wenn Sie die Sperrung einer von Sophos als schädlich eingestuften Website aufheben möchten, fügen Sie die Seite zur Liste der zugelassenen Seiten hinzu. URLs zugelassener Websites werden nicht von der Web-Filterfunktion von Sophos erfasst.

Hinweis: Wenn Download-Scans aktiviert sind und Sie eine Seite mit einem Threat aufrufen, wird der Zugriff auf die Seite gesperrt, auch wenn die Website zugelassen wurde.

So lassen Sie eine Website zu:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** auf die Schaltfläche **Autorisierungen**.
4. Klicken Sie im Dialogfeld **Authorization Manager** auf der Registerkarte **Websites** auf **Hinzufügen**, um eine Website anhand einer der verfügbaren Optionen hinzuzufügen.

   Sie können den Domänennamen, die IP-Adresse oder die IP-Adresse mit Subnetzmaske einer Website hinzufügen.

   Hinweis: Wenn Sie Web Control verwenden, werden Seiten, die von der **Web Control**-Richtlinie gesperrt werden, auch dann blockiert, wenn Sie sie hier zulassen. Wenn Sie Zugriff auf die Website gewähren möchten, müssen Sie sie mit der Filterfunktion von Web Control und in der Antivirus- und HIPS-Richtlinie zulassen. Weitere Informationen zu Web Control finden Sie unter *Informationen zur Web Control-Richtlinie* (Seite 192).

Wenn Sie eine Website bearbeiten oder aus der Liste entfernen möchten, wählen Sie die Website aus und klicken Sie auf **Ändern** oder **Entfernen**.

7.1.6 On-Access-Scans

7.1.6.1 Praxistipps

In diesem Abschnitt wird erläutert, wie Sie On-Access-Scans optimal nutzen können.

Es empfiehlt sich, die Standardeinstellungen für On-Access-Scans zu übernehmen, da so die perfekte Balance zwischen Schutz und Systemleistung gewährleistet wird.

Einige Verschlüsselungsprogramme verhindern die Virenerkennung durch On-Access-Scans. Passen Sie die automatisch gestarteten Prozesse so an, dass Dateien bereits vor On-Access-Scans entschlüsselt werden. Weitere Informationen zum Einsatz der Antivirus- und HIPS-Richtlinie in Kombination mit Verschlüsselungssoftware entnehmen Sie bitte dem Sophos Support-Artikel 12790 *http://www.sophos.de/support/knowledgebase/article/12790.html*.

7.1.6.2 Aktivieren/Deaktivieren der On-Access-Scans

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Standardmäßig scannt Sophos Endpoint Security and Control Dateien, wenn der Anwender versucht, auf sie zuzugreifen und verweigert den Zugriff, wenn sie nicht virenfrei sind.

Möglicherweise möchten Sie On-Access-Scans auf Exchange-Servern oder auf Servern, deren Leistung beeinträchtigt ist, ausschalten. Fassen Sie in diesem Fall die Server zu einer eigenen Gruppe zusammen und ändern Sie die Antivirus- und HIPS-Richtlinie für diese Gruppe wie folgt:

So aktivieren/deaktivieren Sie On-Access-Scans:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.
3. Aktivieren/Deaktivieren Sie im Dialogfeld **On-Access-Scans** das Kontrollkästchen **On-Access-Scans aktivieren** aus.

Wichtig: Wenn Sie On-Access-Scans auf einem Server ausschalten, empfehlen wir Ihnen, auf den entsprechenden Computern geplante Scans einzurichten. Anweisungen zum Einrichten geplanter Scans finden Sie unter *Scannen von Computern zu bestimmten Zeiten* (Seite 108).

7.1.6.3 Ändern der Bedingungen für On-Access-Scans

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können angeben, ob Dateien gescannt werden sollen, wenn sie geöffnet, gespeichert oder umbenannt werden.

So ändern Sie die Bedingungen für On-Access-Scans:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**.
3. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.

4. Klicken Sie im Feld **On-Access-Scans** neben **On-Access-Scans aktivieren** auf die Schaltfläche **Konfigurieren**.
5. Wählen Sie auf der Registerkarte **Scans** im Bereich **Dateien scannen auf** die folgenden Optionen aus.

Scan-Zeitpunkte	Option
Kopieren, Verschieben oder Öffnen einer Datei	**Beim Lesen**
Programm wird gestartet	**Beim Lesen**
Datei wird umbenannt	**Beim Umbenennen**
Datei wird gespeichert	**Beim Schreiben**

7.1.6.4 Scannen auf verdächtige Dateien im Rahmen von On-Access-Scans

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Verdächtige Dateien weisen Merkmale (z.B. dynamischen Dekomprimierungscode) auf, die häufig bei Malware auftreten. Anhand dieser Merkmale kann die Datei jedoch nicht eindeutig als neuartige Malware erkannt werden.

Hinweis: Die Option beschränkt sich auf Sophos Endpoint Security and Control für Windows 2000 und aufwärts.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**.
3. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.

4. Klicken Sie im Feld **On-Access-Scans** neben **On-Access-Scans aktivieren** auf die Schaltfläche **Konfigurieren**.
5. Wählen Sie auf der Registerkarte **Scans** im Bereich **Scannen auf** das Kontrollkästchen **Verdächtige Dateien**.

Wenn eine verdächtige Datei erkannt wird, können Sie die Datei entweder entfernen oder zulassen. Nähere Informationen finden Sie unter *Sofortiges Bereinigen von Computern* (Seite 64) und *Zulassen verdächtiger Objekte* (Seite 107).

7.1.6.5 Ausschließen von Objekten von On-Access-Scans

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können Objekte von On-Access-Scans ausschließen.

Hinweis:

Diese Optionen beschränken sich auf Windows 2000 (und aufwärts), Mac OS X und Linux.

Enterprise Console 5.1 kann auf UNIX-Computern keine On-Access-Scans durchführen.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.

3. Klicken Sie im Feld **On-Access-Scans** auf die Schaltfläche **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Windows-Ausschlüsse**, **Mac-Ausschlüsse** oder **Linux/UNIX-Ausschlüsse**. Um Objekte zu der Liste hinzuzufügen, klicken Sie auf **Hinzufügen** und geben den vollständigen Pfad im Dialogfeld **Objekt ausschließen** ein.

   Die von Scans ausschließbaren Objekte variieren je nach Computertyp. Mehr dazu erfahren Sie unter *Objekte, die von Scans ausgeschlossen werden können* (Seite 111).

Wichtig: Wenn Sie auf der Regiserkarte **Windows-Ausschlüsse** die Option **Remote-Dateien ausschließen** auswählen, werden Dateien, die mit einer überwachten Anwendung, z.B. einem E-Mail-Client, Browser oder Instant Messaging-Client hochgeladen oder angehängt wurden, nicht von Sophos Data Control erfasst. Data Control verwendet die gleichen Ausschlüsse wie der On-Access-Scanner von Sophos Anti-Virus: Wenn das Scannen von Remote-Dateien also deaktiviert wurde, werden keine Remote-Dateien an Data Control gesendet. Diese Einschränkung gilt nicht für die Überwachung von Speichergeräten.

Sie können die Liste mit den Windows-Ausschlüssen in eine Datei exportieren und anschließend in eine andere Richtlinie importieren. Nähere Informationen finden Sie unter *Importieren/Exportieren von Windows-Scan-Ausschlüssen* (Seite 115).

7.1.7 Verhaltensüberwachung

7.1.7.1 Über die Verhaltensüberwachung

Die Verhaltensüberwachung von Sophos schützt Computer mit Windows 2000 und höher im Rahmen von On-Access-Scans vor unbekannten und Zero-Day-Threats sowie verdächtigem Verhalten.

Laufzeiterkennung stoppt Threats, die vor der Ausführung nicht erkannt werden können. Die Verhaltensanalyse stoppt Threats anhand von zwei Methoden in der Laufzeit:

- Erkennunng schädlichen und verdächtigen Verhaltens
- Pufferüberlauferkennung.

Erkennunng schädlichen und verdächtigen Verhaltens

Die Erkennung verdächtigen Verhaltens führt mit Hilfe von Sophos HIPS (Host Intrusion Prevention System) eine dynamische Verhaltensanalyse aller auf dem Computer ausgeführten Programme durch, um Aktivitäten zu erkennen und zu sperren, die wahrscheinlich schädlich sind. Zu verdächtigem Verhalten zählen beispielsweise Änderungen an der Registrierung, die das automatische Ausführen eines Virus zulassen, wenn der Computer neu gestartet wird.

Mit der Option zur Erkennung verdächtigen Verhaltens werden sämtliche Systemprozesse auf aktive Malware hin überwacht. Dabei wird etwa auf verdächtige Schreibvorgänge in der Registrierung oder das Kopieren von Dateien geachtet. Der Administrator kann sich über solches Verhalten benachrichtigen lassen, und/oder die verdächtigen Prozesse können automatisch blockiert werden.

Die Erkennung schädlichen Verhaltens ist die dynamische Analyse aller Programme, die auf einem Computer laufen, um potenziell schädliche Aktivitäten zu erkennen und zu sperren.

Pufferüberlauf-Erkennung

Die Pufferüberlauf-Erkennung ist vor allem im Umgang mit Zero-Day-Exploits wichtig.

Dabei wird eine dynamische Verhaltensanalyse aller ausgeführten Programme durchgeführt, um Pufferüberlauf-Attacken auf laufende Prozesse zu erkennen. Es werden Angriffe entdeckt, die auf Sicherheitslücken in Software und Betriebssystemen abzielen.

7.1.7.2 Verhaltensüberwachung aktivieren

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**.
3. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.

4. Wählen Sie im Dialogfeld **On-Access-Scans** das Kontrollkästchen **Verhaltensüberwachung aktivieren** aus.

7.1.7.3 Erkennung schädlichen Verhaltens

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Die Erkennung schädlichen Verhaltens ist die dynamische Analyse aller Programme, die auf einem Computer laufen, um potenziell schädliche Aktivitäten zu erkennen und zu sperren.

So ändern Sie die Einstellung zur Erkennung und Meldung schädlichen Verhaltens:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**.
3. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.

4. Wählen Sie im Dialogfeld **On-Access-Scans** das Kontrollkästchen **Verhaltensüberwachung aktivieren** aus.
5. Klicken Sie neben **Verhaltensüberwachung aktivieren** auf **Konfigurieren**.
6. Aktivieren Sie das Kontrollkästchen **Erkennung schädlichen Verhaltens**, um Warnmeldungen an den Administrator bei schädlichem Verhalten zu versenden und entsprechende Prozesse zu blockieren.

7.1.7.4 Erkennen verdächtigen Verhaltens

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Mit der Option zur Erkennung verdächtigen Verhaltens werden sämtliche Systemprozesse auf aktive Malware hin überwacht. Dabei wird etwa auf verdächtige Schreibvorgänge in der Registrierung oder das Kopieren von Dateien geachtet. Der Administrator kann sich über

solches Verhalten benachrichtigen lassen, und/oder die verdächtigen Prozesse können automatisch blockiert werden.

So ändern Sie die Einstellung zur Erkennung und Meldung verdächtigen Verhaltens:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**.
3. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.
4. Wählen Sie im Dialogfeld **On-Access-Scans** das Kontrollkästchen **Verhaltensüberwachung aktivieren** aus.
5. Klicken Sie neben **Verhaltensüberwachung aktivieren** auf **Konfigurieren**.
6. Wählen Sie das Kontrollkästchen **Erkennung schädlichen Verhaltens**.
7. Aktivieren Sie das Kontrollkästchen **Erkennung verdächtigen Verhaltens**, um Warnmeldungen an den Administrator bei verdächtigem Verhalten zu versenden und entsprechende Prozesse zu blockieren.
8. Aktivieren Sie das Kontrollkästchen **Nur melden, nicht blockieren**, um Warnmeldungen an den Administrator bei verdächtigem Verhalten zu versenden, entsprechende Prozesse jedoch nicht zu blockieren.

Es empfiehlt sich, die Erkennung verdächtiger Dateien zu aktivieren. Nähere Informationen finden Sie unter *Scannen auf verdächtige Dateien im Rahmen von On-Access-Scans* (Seite 102) und *Scannen auf verdächtige Dateien im Rahmen von geplanten Scans* (Seite 109).

7.1.7.5 Erkennen von Pufferüberläufen

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Die „Pufferüberlauf-Erkennung“ führt eine dynamische Verhaltensanalyse aller ausgeführten Programme durch, um Pufferüberlauf-Attacken auf laufende Prozesse zu erkennen.

So ändern Sie die Einstellung zur Erkennung und Meldung von Pufferüberläufen:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**.
3. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.

4. Wählen Sie im Dialogfeld **On-Access-Scans** das Kontrollkästchen **Verhaltensüberwachung aktivieren** aus.
5. Klicken Sie neben **Verhaltensüberwachung aktivieren** auf **Konfigurieren**.
   - Aktivieren Sie das Kontrollkästchen **Pufferüberläufe erkennen** und deaktivieren Sie die Option **Nur melden, nicht blockieren**, um Warnmeldungen an den Administrator bei Pufferüberläufen zu versenden und Pufferüberläufe zu blockieren.
   - Aktivieren Sie die Kontrollkästchen **Pufferüberläufe erkennen** und **Nur melden, nicht blockieren**, um Warnmeldungen an den Administrator bei Pufferüberläufen zu versenden, Pufferüberläufe jedoch nicht zu blockieren.

7.1.7.6 Zulassen verdächtiger Objekte

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wenn Sie eine oder mehrere HIPS-Optionen aktiviert haben (z.B. Erkennung verdächtigen Verhaltens, Erkennung von Pufferüberläufen oder Erkennung verdächtiger Dateien), jedoch einige der Objekte verwenden möchten, können Sie sie folgendermaßen zulassen:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**.
3. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.
4. Klicken Sie auf **Autorisierungen**.

   Das Dialogfeld **Authorization Manager** wird angezeigt.
5. Klicken Sie auf die Registerkarte, die dem erkannten Verhalten entspricht (z.B. Pufferüberlauf).
   - Wenn Sie ein erkanntes Programm zulassen möchten, suchen Sie es in der Liste **Bekannt** und verschieben Sie es von dort in die Liste **Zugelassen**.
   - Wenn Sie Objekte zulassen möchten, die Sophos Endpoint Security and Control *nicht* als verdächtig eingestuft, klicken Sie auf die Option **Neuer Eintrag**. Suchen Sie nach dem Objekt und nehmen Sie es in die Liste **Zugelassen** auf.

Wenn Sie ein Objekt aus der Liste entfernen möchten, wählen Sie das Objekt und klicken Sie auf **Eintrag löschen**. Wenn Sie das Objekt zugelassen haben, wird es wieder blockiert, wenn Sie es aus der Liste entfernen. Verwenden Sie diese Option also nur, wenn Sie sicher sind, dass das Objekt nicht zugelassen werden muss. Diese Option löscht das Objekt nicht von der Festplatte.

7.1.8 Geplante Scans

7.1.8.1 Scannen von Computern zu bestimmten Zeiten

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Computer können zu festgesetzten Zeiten gescannt werden.

Hinweis: Auf Mac-Computern werden geplante Scans nur ab Sophos Anti-Virus, Version 8.0 unterstützt.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Geplante Scans** auf **Hinzufügen**.
4. Geben Sie im Dialogfeld **Einstellungen zu geplanten Scans** einen Namen für den geplanten Scan ein. Wählen Sie die Objekte aus, die gescannt werden sollen (standardmäßig werden alle lokalen Festplatten oder bereitgestellten Dateisysteme gescannt). Wählen Sie den gewünschten Scanzeitpunkt (Datum und Uhrzeit) aus.
5. Wenn Sie andere Scan-Optionen ändern oder diesen Scan zum Bereinigen von Computern konfigurieren möchten, klicken Sie unten im Dialogfeld auf **Konfigurieren**.

   Mehr zu den Optionen für geplante Scans erfahren Sie unter *Ändern der Einstellungen für geplante Scans* (Seite 108).

Hinweis: Wenn beim Scan Threat-Komponenten im Speicher erkannt werden und Sie keine automatische Bereinigung für den Scan eingerichtet haben, wird der Scan angehalten und ein Alert wird an Enterprise Console gesendet. Wenn der Scan fortgesetzt wird, könnte sich der Threat ausbreiten. Sie müssen den Threat zunächst bereinigen, bevor Sie den Scan erneut ausführen können.

7.1.8.2 Ändern der Einstellungen für geplante Scans

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So können Sie die Einstellungen für geplante Scans ändern:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Geplante Scans** die gewünschten Einstellungen vor.

   Sie können die folgenden Änderungen vornehmen:

   - Wenn Sie die Dateitypen ändern möchten, die von *allen* geplanten Scans erfasst werden, klicken Sie auf **Erweiterungen und Ausschlüsse**.
   - Wenn Sie spezifische Einstellungen einer Scanfunktion ändern möchten (z.B. Scan-Objekte, Scan-Zeit, Scan-Optionen, Bereinigung), markieren Sie den Scan und klicken auf **Ändern**. Klicken Sie dann im Dialogfeld **Einstellungen zu geplanten Scans** auf **Konfigurieren**.

   Hinweis: Nähere Informationen zu Scan-Optionen finden Sie unter *Scannen auf verdächtige Dateien im Rahmen von On-Access-Scans* (Seite 102), *Scannen auf Adware und PUA* (Seite 96) und *Scannen von Archivdateien* (Seite 113). Bereinigungs-Optionen werden unter *Einstellungen der automatischen Bereinigung für geplante Scans* (Seite 67) näher erläutert.

7.1.8.3 Scannen auf verdächtige Dateien im Rahmen von geplanten Scans

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Verdächtige Dateien weisen Merkmale (z.B. dynamischen Dekomprimierungscode) auf, die häufig bei Malware auftreten. Anhand dieser Merkmale kann die Datei jedoch nicht eindeutig als neuartige Malware erkannt werden.

Hinweis: Die Option beschränkt sich auf Sophos Endpoint Security and Control für Windows 2000 und aufwärts.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**.
3. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet.

4. Wählen Sie im Dialogfeld **Geplante Scans** einen vorhandenen Scan aus und klicken Sie auf **Bearbeiten**.

5. Klicken Sie neben **Einstellungen zu Scans und Bereinigung ändern** auf **Konfigurieren**.

   Das Dialogfeld **Scan- und Bereinigungs-Einstellungen** wird geöffnet.

6. Wählen Sie auf der Registerkarte **Scans** im Bereich **Dateien scannen auf** das Kontrollkästchen **Verdächtige Dateien**.

Wenn eine verdächtige Datei erkannt wird, können Sie die Datei entweder entfernen oder zulassen. Nähere Informationen finden Sie unter *Sofortiges Bereinigen von Computern* (Seite 64) und *Zulassen verdächtiger Objekte* (Seite 107).

7.1.8.4 Ausschließen von Objekten von geplanten Scans

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können Objekte von geplanten Scans ausschließen.

Hinweis:

Die Einstellungen für die ausgeschlossenen Objekte für geplante Scans treffen auch für vollständige Systemüberprüfungen zu, die von der Konsole gestartet werden, und für Scans über die Option „Meinen Computer scannen“ auf Netzwerkcomputern. Mehr dazu erfahren Sie unter *Sofort-Scans* (Seite 63).

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Das Dialogfeld **Antivirus- und HIPS-Richtlinie** wird geöffnet. Klicken Sie im Fensterbereich **Geplante Scans** auf **Erweiterungen und Ausschlüsse**.
4. Klicken Sie auf die Registerkarte **Windows-Ausschlüsse**, **Linux-/UNIX-Ausschlüsse** oder**Mac-Ausschlüsse**. Um Objekte zu der Liste hinzuzufügen, klicken Sie auf **Hinzufügen** und geben den vollständigen Pfad im Dialogfeld **Objekt ausschließen** ein.

   Die von Scans ausschließbaren Objekte variieren je nach Computertyp. Mehr dazu erfahren Sie unter *Objekte, die von Scans ausgeschlossen werden können* (Seite 111).

Sie können die Liste mit den Windows-Ausschlüssen in eine Datei exportieren und anschließend in eine andere Richtlinie importieren. Weitere Informationen finden Sie unter *Importieren/Exportieren von Windows-Scan-Ausschlüssen* (Seite 115).

7.1.9 Scan-Optionen

7.1.9.1 Objekte, die von Scans ausgeschlossen werden können

Objekte, die von Scans ausgeschlossen werden können, variieren je nach Betriebssystem.

Windows

Unter Windows 2000 und höher können Sie Laufwerke, Ordner und Dateien ausschließen.

Sie können die Platzhalter * und ? benutzen.

Der Platzhalter ? kann nur für Dateinamen oder Erweiterungen benutzt werden. Er ersetzt in der Regel ein einziges Zeichen. Am Ende eines Dateinamens kann das Fragezeichen jedoch auch ein fehlendes Zeichen ersetzen. Beispiel: Die Eingabe von „datei??.txt“ dient als Ersatz für „datei.txt“, „datei1.txt“ sowie „datei12.txt“, jedoch nicht „datei123.txt“.

Der Platzhalter * kann nur für Dateinamen oder -erweiterungen in der Form [Dateiname].* oder *.[Erweiterung] verwendet werden. Beispiel: Die Eingabe von „datei*.txt“, „datei.txt*“ und „datei.*txt“ ist nicht zulässig.

Weitere Details werden im Abschnitt „Sophos Anti-Virus“ in der Hilfe zu Sophos Endpoint Security and Control beschrieben.

Mac OS X

Unter Mac OS X können Sie Dateien, Ordner und Volumes ausschließen.

Sie können Objekte auschließen, indem Sie einen Schrägstrich/doppelten Schrägstrich an das auszuschließende Objekt anhängen bzw. vor das Objekt setzen.

Nähere Informationen entnehmen Sie bitte der Hilfe zu Sophos Anti-Virus für Mac.

Linux oder UNIX

Unter Linux und UNIX können Sie Verzeichnisse und Dateien ausschließen, indem Sie einen Pfad angeben (mit oder ohne Platzhalter).

Hinweis: Enterprise Console unterstützt nur Pfad-basierte Linux- und UNIX-Ausnahmen. Sie können außerdem andere Arten von Ausnahmen direkt auf den verwalteten Computern einrichten. Sie können dann reguläre Ausdrücke verwenden und Dateitypen und Dateisysteme ausschließen. Anweisungen dazu finden Sie im *Benutzerhandbuch zu Sophos Anti-Virus für Linux* oder für *Sophos Anti-Virus für UNIX*.

Wenn Sie eine weitere Pfad-basierte Ausnahme auf einem verwalteten Linux- oder UNIX-Computer einrichten, wird dieser Computer der Konsole als von der Gruppenrichtlinie abweichend gemeldet.

7.1.9.2 Ändern der Scan-Objekte

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Standardmäßig scannt Sophos Endpoint Security and Control Dateitypen, die für Viren anfällig sind. Sie können weitere Dateitypen (Scan-Objekte) scannen lassen oder auch bestimmte Dateitypen von Scans ausschließen.

Die standardmäßig gescannten Dateitypen sind vom Betriebssystem abhängig und ändern sich bei Produkt-Updates. Sie können eine Liste der Dateitypen ansehen, wenn Sie zu einem Computer mit dem entsprechenden Betriebssystem gehen, Sophos Endpoint Security and Control oder Sophos Anti-Virus öffnen und dort die Konfigurationsseite mit den Erweiterungen aufrufen.

Hinweis:

Diese Optionen sind nur für Windows-Computer relevant.

Änderungen an Mac OS X-Systemen können Sie über Sophos Update Manager vornehmen, einem mit Sophos Anti-Virus für Mac OS X ausgelieferten Tool. Zum Starten von Sophos Update Manager unter Mac OS X öffnen Sie ein **Finder**-Fenster und suchen den Ordner „Sophos Anti-Virus:ESOSX“. Doppelklicken Sie auf **Sophos Update Manager**. Weitere Details werden in der Hilfe zu Sophos Update Manager aufgeführt.

Die Virenschutzeinstellungen auf Linux-Computern können Sie über die Befehle „savconfig“ und „savscan“ändern. Anweisungen hierzu finden Sie im Benutzerhandbuch für Sophos Anti-Virus für Linux.

Die Virenschutzeinstellungen für UNIX-Computer können Sie über den Befehl „savscan“ ändern. Anweisungen hierzu finden Sie im Benutzerhandbuch für Sophos Anti-Virus für UNIX.

So lassen sich die Scan-Objekte ändern:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Stellen Sie die Optionen im Dialogfeld **Antivirus- und HIPS-Richtlinie** folgendermaßen ein:

   - Stellen Sie bei der Konfiguration von On-Access-Scans sicher, dass im Feld **On-Access-Scans** die Option **On-Access-Scans aktivieren** ausgewählt ist. Klicken Sie neben dem Kontrollkästchen auf die Schaltfläche **Konfigurieren**.
   - Klicken Sie zur Konfiguration von geplanten Scans Sie im Bereich **Geplante Scans** auf **Erweiterungen und Ausschlüsse**.

4. Wählen Sie auf der Registerkarte **Erweiterungen** die Option **Ausführbare und infizierbare Dateien scannen**.

   - Um weitere Dateitypen zu scannen, klicken Sie auf **Hinzufügen** und geben im Feld **Erweiterung** die entsprechende Dateinamenserweiterung ein, z.B. PDF.
   - Um standardmäßig gescannte Dateitypen auszuschließen, klicken Sie auf **Ausschließen**. Das Dialogfeld **Erweiterungen ausschließen** wird angezeigt. Geben Sie die Dateierweiterung ein.

Standardmäßig werden Dateien ohne Erweiterung gescannt.

Hinweis: Sie können auch alle Dateien scannen lassen; dies beeinträchtigt jedoch die Leistung des Computers.

7.1.9.3 Scannen von Archivdateien

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Hinweis: Durch das Scannen von Archivdateien verlangsamt sich der Scan-Vorgang. Archive müssen jedoch in der Regel nicht gescannt werden. Auch wenn Sie diese Option nicht auswählen und versuchen, auf eine Datei zuzugreifen, die aus dem Archiv entpackt wurde, wird die entpackte Datei gescannt. Es empfiehlt sich daher nicht, diese Option zu wählen.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Geplante Scans** auf **Hinzufügen** (oder markieren Sie einen bestehenden Scan und klicken Sie auf **Ändern**).
4. Geben Sie im Dialogfeld **Einstellungen zu geplanten Scans** Ihre Einstellungen ein und klicken Sie dann auf **Konfigurieren** (unten in diesem Fenster).
5. Wählen Sie im Dialogfeld **Scan- und Bereinigungs-Einstellungen** auf der Registerkarte **Scans** unter *Sonstige Scan-Einstellungen* die Option **Archivdateien scannen**. Klicken Sie auf **OK**.

7.1.9.4 Scannen auf Rootkits

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Beim Durchführen einer vollständigen Systemüberprüfung wird auch auf Rootkits gescannt. (Mehr dazu erfahren Sie unter *Sofort-Scans* (Seite 63)). Wenn Sie die Einstellungen für einen geplanten Scan ändern möchten, verfahren Sie wie folgt.

Hinweis: Die Option beschränkt sich auf Sophos Endpoint Security and Control für Windows 2000 und aufwärts.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten. Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Geplante Scans** auf **Hinzufügen** (oder markieren Sie einen bestehenden Scan und klicken Sie auf **Ändern**).
4. Geben Sie im Dialogfeld **Einstellungen für geplante Scans** Ihre Einstellungen ein und klicken Sie auf **Konfigurieren**.
5. Wählen Sie im Dialogfeld **Einstellungen zu Scans und Bereinigung ändern** auf der Registerkarte **Scans** im Bereich **Dateien scannen auf** das Kontrollkästchen **Rootkits**. Klicken Sie auf **OK**.

7.1.9.5 Scannen des Systemspeichers

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Endpoint Security and Control für Windows kann den Systemspeicher auf Threats scannen. Der *Systemspeicher* wird vom Betriebssystem genutzt. Der Systemspeicher kann in Endpoint Security and Control in regelmäßigen Abständen im Hintergrund bei aktivierten On-Access-Scans oder im Rahmen eines geplanten Scans gescannt werden.

So können Sie den Systemspeicher scannen:

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Stellen Sie die Optionen im Dialogfeld **Antivirus- und HIPS-Richtlinie** folgendermaßen ein:

   - **On-Access-Überprüfung**

     Stellen Sie bei der Konfiguration von On-Access-Scans sicher, dass im Feld **On-Access-Scans** die Option **On-Access-Scans aktivieren** ausgewählt ist. Klicken Sie neben dem Kontrollkästchen auf die Schaltfläche **Konfigurieren**.

     Wählen Sie auf der Registerkarte **Scans** im Bereich **Sonstige Scan-Optionen** das Kontrollkästchen **Systemspeicher scannen**.

- **Geplante Scans**

  Klicken Sie zum Konfigurieren von geplanten Scans im Bereich **Geplante Scans** auf **Hinzufügen** (oder wählen Sie einen bestehenden Scan und klicken Sie auf **Ändern**).

  Geben Sie im Dialogfeld **Einstellungen für geplante Scans** Ihre Einstellungen ein und klicken Sie auf **Konfigurieren**.

  Aktivieren Sie im Dialogfeld **Scan- und Bereinigungs-Einstellungen** auf der Registerkarte **Scans** im Bereich **Sonstige Scanoptionen** das Kontrollkästchen **Systemspeicher scannen**.

Hinweis: Wenn Sie die automatische Bereinigung von von On-Access-Scans erkannten Viren aktiviert haben, wird unter Umständen eine vollständige Systemüberprüfung eingeleitet, um *alle* Viren vom Computer zu bereinigen. Dieser Vorgang kann viel Zeit in Anspruch nehmen.

7.1.9.6 Scannen mit niedriger Priorität

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können einen benutzerdefinierten Scan mit niedriger Priorität ausführen, um die Auswirkungen auf Anwendungen zu minimieren.

Hinweis: Die Option beschränkt sich auf Sophos Endpoint Security and Control für Windows Vista und aufwärts.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten. Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Geplante Scans** auf **Hinzufügen** (oder markieren Sie einen bestehenden Scan und klicken Sie auf **Ändern**).
4. Geben Sie im Dialogfeld **Einstellungen für geplante Scans** Ihre Einstellungen ein und klicken Sie auf **Konfigurieren**.
5. Aktivieren Sie im Dialogfeld **Scan- und Bereinigungs-Einstellungen** auf der Registerkarte **Scans** im Bereich *Sonstige Scanoptionen* das Kontrollkästchen **Scan mit niedriger Priorität ausführen**. Klicken Sie auf **OK**.

7.1.9.7 Importieren/Exportieren von Windows-Scan-Ausschlüssen

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können die Liste mit den Windows-Ausschlüssen zu On-Access-Scans oder geplanten Scans in eine Datei exportieren und anschließend in eine andere Richtlinie importieren.

1. Prüfen Sie, welche Antivirus- und HIPS-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Verfahren Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** wie folgt:
   - Stellen Sie zum Importieren/Exportieren von Ausschlüssen zu On-Access-Scans sicher, dass die Option **On-Access-Scans aktivieren** aktiviert wurde und klicken Sie neben dem Kontrollkästchen auf die Schaltfläche **Konfigurieren**.
   - Klicken Sie zum Importieren/Exportieren von Ausschlüssen von geplanten Scans im Bereich **Geplante Scans** auf **Erweiterungen und Ausschlüsse**.
4. Klicken Sie auf der Registerkarte **Windows-Ausschlüsse** auf **Exportieren** oder **Importieren**.

7.2 Konfigurieren der Firewall-Richtlinie

7.2.1 Basiskonfiguration der Firewall

7.2.1.1 Einrichten einer Firewall-Richtlinie

Die Firewall ist standardmäßig aktiviert und sperrt unnötigen Datenverkehr. Daher sollten regelmäßig genutzte Anwendungen in der Firewall zugelassen werden. Testen Sie die Einstellungen vor der Installation. Weitere Hinweise dazu finden Sie in der *Richtlinienanleitung* zu Sophos Enterprise Console.

Die Firewall-Einstellungen werden im Sophos Support-Artikel 57756 (*http://www.sophos.de/support/knowledgebase/article/57756.html*) näher beschrieben.

Nähere Informationen zum Vermeiden von Netzwerkbrücken finden Sie unter *Device Control* (Seite 171).

Wichtig: Wenn Sie eine neue oder aktualisierte Richtlinie auf Computer übertragen, werden Anwendungen, die von der alten Richtlinie zugelassen wurden, eventuell kurzfristig gesperrt, bis die neue Richtlinie in vollem Umfang angewendet wird. Sie sollten die Benutzer im Netzwerk über die Einführung neuer Richtlinien benachrichtigen.

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 17) entnehmen.

So richten Sie eine Firewall-Richtlinie ein:

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Firewall**.
2. Doppelklicken Sie auf die **Standardrichtlinie**, um sie zu bearbeiten.

   Der **Firewall-Richtlinienassistent** wird geöffnet. Befolgen Sie die Anweisungen auf dem Bildschirm. Diverse Optionen werden unten näher erläutert.

3. Machen Sie auf der Seite **Firewall konfigurieren** Angaben zum Standort:

   - Wählen Sie **Ein Standort**, wenn sich Computer immer im Netzwerk befinden, z.B. Desktop Computer.
   - Wählen Sie **Zwei Standorte**, wenn die Firewall unterschiedliche Einstellungen je nach Standort des Computers aufweisen soll, z.B. im Büro (im Firmennetzwerk) oder extern (nicht im Firmennetzwerk). Für Laptops empfiehlt sich die Auswahl mehrerer Standorte.

4. Geben Sie auf der Seite **Arbeitsmodus** an, wie die Firewall eingehenden und ausgehenden Datenfluss behandeln soll.

Modus	Beschreibung
Eingehenden und ausgehenden Datenfluss blockieren	■ Standard. Bietet den höchsten Grad an Sicherheit. ■ Nur der unbedingt erforderliche Datenfluss wird von der Firewall zugelassen, und die Identität der Anwendungen wird mittels Prüfsummen authentifiziert. ■ Klicken Sie zum Zulassen der Kommunikation häufig eingesetzter Anwendungen in Ihrem Unternehmen über die Firewall auf **Vertrauen**. Nähere Informationen finden Sie unter *Informationen zum Zulassen von Anwendungen* (Seite 125).
Eingehenden Datenfluss blockieren, ausgehenden Datenfluss erlauben	■ Diese Option bietet weniger Sicherheit als **Eingehenden und ausgehenden Datenfluss blockieren**. ■ Computer können ohne die Erstellung besonderer Regeln auf das Netzwerk und Internet zugreifen. ■ Alle Anwendungen dürfen über die Firewall kommunizieren.
Überwachen	■ Überträgt die erstellten Regeln auf Datenfluss im Netzwerk. Wenn dem Datenfluss keine passende Regel zugewiesen wurde, wird dies der Konsole gemeldet. Wenn es sich um ausgehenden Datenfluss handelt, wird er zugelassen. ■ Auf diese Weise können Sie sich einen Überblick über die Verkehrssituation im Netzwerk verschaffen und geeignete Regeln erstellen, bevor Sie die Firewall für alle Computer wirksam machen. Nähere Informationen finden Sie unter *Informationen zum Überwachungsmodus* (Seite 118).

5. Wählen Sie auf der Seite **Datei- und Druckerfreigabe** die Option **Datei- und Druckerfreigabe zulassen**, wenn Sie anderen Computern den Zugriff auf Drucker und Freigaben im Netzwerk ermöglichen möchten.

Nach der Konfiguration der Firewall können Sie Firewall-Ereignisse (z.B. von der Firewall gesperrte Anwendungen) in der **Firewall – Ereignisanzeige** aufrufen. Mehr dazu erfahren Sie unter *Anzeige von Firewall-Ereignissen* (Seite 214).

Im Dashboard wird die Anzahl der Computer angezeigt, deren Ereignisanzahl in den vergangenen 7 Tagen einen festgelegten Höchstwert überschritten hat.

7.2.1.2 Informationen zum Überwachungsmodus

Sie können den Überwachungsmodus auf Testcomputern aktivieren, auf denen Sie in der Firewall-Ereignisanzeige den Datenfluss und die Nutzung von Anwendungen beobachten können.

In der Ereignisanzeige können Sie Regeln zum Zulassen oder Blockieren von Datenfluss, Anwendungen und Prozessen erstellen. Dies wird unter *Erstellen einer Firewall-Ereignisregel* (Seite 122) beschrieben.

Hinweis: Wenn Sie in der Firewall-Ereignisanzeige eine Regel erstellen und sie zur Firewall-Richtlinie hinzufügen, ändert sich der Firewall-Modus von **Überwachen** in **Benutzerdefiniert**.

Wenn unbekannter Datenfluss nicht standardmäßig zugelassen werden soll, betreiben Sie die Firewall im *interaktiven Modus*.

Im interaktiven Modus gibt der Benutzer an, ob Datenfluss und Anwendungen, denen keine Regel zugewiesen wurde, zugelassen oder gesperrt werden sollen. Details entnehmen Sie bitte *Allgemeine Informationen* (Seite 124) und anderen Abschnitten im Kapitel „Arbeiten im interaktiven Modus“.

7.2.1.3 Hinzufügen und Zulassen einer Anwendung

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Vertrauenswürdige Anwendungen erhalten uneingeschränkten Vollzugriff auf das Netzwerk und das Internet.

So können Sie eine Anwendung in die Firewall-Richtlinie aufnehmen und zulassen:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie auf der Seite **Arbeitsmodus** des **Firewall-Richtlinienassistenten** auf **Vertrauen**.

   Das Dialogfenster **Firewall-Richtlinie** wird angezeigt.
4. Klicken Sie auf **Hinzufügen**.

   Das Dialogfenster **Firewall-Richtlinie – Zuverlässige Anwendung hinzufügen** wird angezeigt.
5. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Anwendungsereignisse angezeigt werden sollen.

   Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt Ihren eigenen Zeitraum bestimmen.
6. Wenn Sie Anwendungsereignisse eines bestimmten Typs aufrufen möchten, wählen Sie den gewünschten Typ im Dropdown-Menü **Ereignistyp** aus.

7. Wenn Sie Anwendungsereignisse für eine bestimmte Datei aufrufen möchten, geben Sie in das Feld **Dateiname** den entsprechenden Namen ein.

   Wenn Sie keine spezifischen Angaben machen, werden Anwendungsereignisse für alle Dateien angezeigt.

   Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.

8. Klicken Sie zur Anzeige einer Anwendungsereignisliste auf **Suche**.
9. Wählen Sie ein Anwendungsereignis aus der Liste und klicken Sie auf **OK**.

Die Anwendung wird in die Firewall-Richtlinie aufgenommen und als **vertrauenswürdig** gekennzeichnet.

7.2.1.4 Zulassen des gesamten Dateiflusses in einem lokalen Netzwerk

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So lassen Sie den gesamten Datenfluss zwischen Computern in einem lokalen Netzwerk (Local Area Network) zu:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie in der **Datei- und Druckerfreigabe** auf der Seite des **Firewall-Richtlinien-Assistenten** die Option **Benutzerdefinierte Einstellungen verwenden** und klicken Sie anschließend auf **Benutzerdefiniert**.
4. Aktivieren Sie für ein Netzwerk in der Liste **LAN-Einstellungen** die Option **Zuverlässig**.

Hinweise

- Wenn Sie den gesamten Datenverkehr zwischen den Computern in einem LAN zulassen, werden automatisch auch Dateien und Drucker zur gemeinsamen Nutzung freigegeben.

7.2.1.5 Zulassen der Datei- und Druckerfreigabe

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So lassen Sie die Drucker- und Dateifreigabe im Netzwerk zu:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie auf der Seite **Datei- und Druckerfreigabe** des **Firewall-Richtlinien-Assistenten** die Option **Datei- und Druckerfreigabe zulassen**.

7.2.1.6 Zulassen der flexiblen Steuerung der Datei- und Druckerfreigabe

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wenn Sie die Datei- und Druckerfreigabe in den Unternehmensnetzwerken flexibler steuern können möchten (z.B. unidirektionalen NetBIOS-Traffic), können Sie wie folgt vorgehen:

1. Lassen Sie die Datei- und Druckerfreigabe auf den LANs (Local Area Networks) zu, die nicht in der Liste mit den **LAN-Einstellungen** aufgeführt sind. So wird der NetBIOS-Traffic auf diesen LANs von den Firewall-Regeln erfasst.
2. Erstellen Sie globale Regeln hoher Priorität, die die Kommunikation zu und von den Hosts mit den passenden NetBIOS-Ports und Protokollen ermöglichen. Es empfiehlt sich, globale Regeln zu erstellen und unerwünschten Traffic der Datei- und Druckerfreigabe zu sperren, anstatt ihn von der Standardregel steuern zu lassen.

So lassen Sie die Datei- und Druckerfreigabe auf den LANs (Local Area Networks) zu, die nicht in der Liste mit den **LAN-Einstellungen** aufgeführt sind:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie in der **Datei- und Druckerfreigabe** auf der Seite des **Firewall-Richtlinien-Assistenten** die Option **Benutzerdefinierte Einstellungen verwenden** und klicken Sie anschließend auf **Benutzerdefiniert**.
4. Deaktivieren Sie die Option **Datei- und Druckerfreigabe für andere Netzwerke sperren**.

7.2.1.7 Sperren unerwünschter Datei- und Druckerfreigabe

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.

- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So sperren Sie die Datei- und Druckerfreigabe auf den LANs (Local Area Networks), die nicht in der Liste mit den **LAN-Einstellungen** auf der Registerkarte **LAN** aufgeführt sind:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie in der **Datei- und Druckerfreigabe** auf der Seite des **Firewall-Richtlinien-Assistenten** die Option **Benutzerdefinierte Einstellungen verwenden** und klicken Sie anschließend auf **Benutzerdefiniert**.
4. Aktivieren Sie die Option **Datei- und Druckerfreigabe für andere Netzwerke sperren**.

7.2.1.8 Erstellen einer Firewall-Ereignisregel

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können Regeln für alle Firewall-Ereignisse erstellen. Eine Ausnahme bilden Ereignisse vom Typ „Modifizierter Speicher“.

So können Sie eine Firewall-Ereignisregel erstellen:

1. Klicken Sie im Menü **Ereignisse** auf **Firewall-Ereignisse**.
2. Wählen Sie im Dialogfeld **Firewall – Ereignisanzeige** ein Ereignis für die Anwendung aus, für die eine Regel erstellt werden soll, und klicken Sie auf **Regel erstellen**.
3. Wählen Sie im Dialogfeld eine Option aus, die für die Anwendung übernommen werden soll.
4. Bestimmen Sie, ob die Regel nur für den primären, den sekundären, oder für beide Standorte gelten soll. Wenn Sie den sekundären Standort oder beide Standorte auswählen, wird die Regel nur auf Richtlinien übertragen, für die ein sekundärer Standort konfiguriert wurde. Klicken Sie auf **OK**.

   Hinweis: Die Ereignisse vom Typ „Neue Anwendung“ und „Geänderte Anwendung“ sind standortunabhängig und fügen Prüfsummen hinzu, die von beiden Standorten genutzt werden. Für diese Ereignisse lässt sich kein Standort auswählen.
5. Wählen Sie aus der Liste der Firewall-Richtlinien die Richtlinie(n) aus, die Sie in die Regel aufnehmen möchten. Klicken Sie auf **OK**.

   Hinweis: Einer Richtlinie, die außerhalb der aktiven Teilverwaltungseinheit wirksam ist, lässt sich keine Regel zuweisen.

Hinweis: Wenn Sie eine Anwendungsregel anhand der erweiterten Firewall-Richtlinieneinstellungen aus einer Firewall-Richtlinie heraus erstellen möchten, lesen Sie *Erstellen einer Anwendungsregel aus einer Firewall-Richtlinie* (Seite 142).

7.2.1.9 Vorübergehende Deaktivierung der Firewall

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Die Firewall ist standardmäßig deaktiviert. Unter bestimmten Umständen (z.B. aus Wartungsgründen oder zur Fehlersuche) muss die Firewall vorübergehend deaktiviert werden.

So deaktivieren Sie die Firewall für eine Computergruppe:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Firewall**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Der **Firewall-Richtlinienassistent** wird geöffnet.

3. Auf der Startseite führen Sie folgende Schritte durch:

   - Wenn die Firewall sowohl an allen festgelegten Standorten (also primäre und sekundäre) deaktiviert werden soll, klicken Sie auf **Weiter**. Wählen Sie auf der Seite **Firewall konfigurieren** die Option **Gesamten Verkehr zulassen (Firewall deaktiviert)**. Beenden Sie den Assistenten.
   - Wenn Sie die Firewall nur an einem Standort (primär oder sekundär) deaktivieren wollen, klicken Sie auf **Erweiterte Einstellungen**. Wählen Sie im Fenster **Firewall-Richtlinie** neben **Primärer Standort** oder **Sekundärer Standort** die Option **Gesamten Datenfluss zulassen**. Klicken Sie auf **OK**. Beenden Sie den **Firewall-Richtlinienassistenten**.

Die Computer bleiben so lange ungeschützt, bis die Firewall wieder aktiviert wird. Zum Aktivieren der Firewall deaktivieren Sie das Kontrollkästchen **Gesamten Datenfluss zulassen**.

7.2.2 Erweiterte Konfiguration der Firewall

7.2.2.1 Öffnen der erweiterten Konfiguration

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.

- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wenn Sie die Firewall ausführlicher konfigurieren möchten, nutzen Sie die erweiterten Konfigurationseinstellungen.

So gelangen Sie zur erweiterten Konfiguration:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.

7.2.2.2 Arbeiten im interaktiven Modus

7.2.2.2.1 Allgemeine Informationen

Im interaktiven Modus wird auf dem Endpoint ein Lerndialog angezeigt, wenn eine unbekannte Anwendung oder ein unbekannter Dienst Netzwerkzugriff anfordert. Der Benutzer kann angeben, ob Datenfluss zugelassen oder gesperrt werden soll oder ob eine Regel dafür erstellt werden soll.

7.2.2.2.2 Aktivieren des interaktiven Modus

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können die Firewall im interaktiven Modus betreiben. Der Benutzer wird dabei gefragt, wie mit dem erkannten Datenverkehr umgegangen werden soll. Weitere Informationen finden Sie unter *Allgemeine Informationen* (Seite 124).

So können Sie auf Computergruppen den interaktiven Modus der Firewall aktivieren:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
4. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
5. Klicken Sie auf der Registerkarte **Allgemein** unter **Arbeitsmodus** auf **Interaktiv**.

7.2.2.2.3 Auswählen eines nicht interaktiven Modus

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Es gibt zwei nicht interaktive Modi:

- Standardmäßig zulassen
- Standardmäßig sperren

In den nicht interaktiven Modi regelt die Firewall den Datenfluss automatisch anhand festgelegter Regeln. (Ausgehender) Netzwerk-Datenfluss ohne passende Regeln wird entweder zugelassen oder gesperrt.

So können Sie auf Computergruppen in einen nicht interaktiven Modus der Firewall wechseln:

1. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Allgemein**.
5. Klicken Sie im Bereich **Arbeitsmodus** auf **Standardmäßig zulassen** bzw. **Standardmäßig sperren**.

7.2.2.3 Konfigurieren der Firewall

7.2.2.3.1 Informationen zum Zulassen von Anwendungen

Die Firewall blockiert aus Sicherheitsgründen Datenverkehr von Anwendungen auf dem Computer, die nicht erkannt wurden. Häufig verwendete Anwendungen in Ihrem Unternehmen werden jedoch möglicherweise gesperrt und einige Benutzer könnten dadurch von ihrer Arbeit abgehalten werden.

Sie können diese Anwendungen *zulassen*, damit sie über die Firewall kommunizieren können. Vertrauenswürdige Anwendungen erhalten uneingeschränkten Vollzugriff auf das Netzwerk und das Internet.

Hinweis: Über Anwendungsregeln können Sie Bedingungen für die Ausführung der Anwendung festlegen und somit die Sicherheit erhöhen. Anweisungen hierzu finden Sie im Abschnitt *Erstellen einer Anwendungsregel* (Seite 141) und anderen Themen zu *Anwendungsregeln*.

7.2.2.3.2 Aufnahme einer Anwendung in eine Firewall-Richtlinie

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So können Sie eine Anwendung in eine Firewall-Richtlinie aufnehmen:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
4. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
5. Klicken Sie auf die Registerkarte **Anwendungen**.
6. Klicken Sie auf **Hinzufügen**.

   Das Dialogfenster **Firewall-Richtlinie – Anwendung hinzufügen** wird angezeigt.
7. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Anwendungsereignisse angezeigt werden sollen.

   Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt Ihren eigenen Zeitraum bestimmen.
8. Wenn Sie Anwendungsereignisse eines bestimmten Typs aufrufen möchten, wählen Sie den gewünschten Typ im Dropdown-Menü **Ereignistyp** aus.
9. Wenn Sie Anwendungsereignisse für eine bestimmte Datei aufrufen möchten, geben Sie in das Feld **Dateiname** den entsprechenden Namen ein.

   Wenn Sie keine spezifischen Angaben machen, werden Anwendungsereignisse für alle Dateien angezeigt.

   Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.
10. Klicken Sie zur Anzeige einer Anwendungsereignisliste auf **Suche**.
11. Wählen Sie ein Anwendungsereignis aus der Liste und klicken Sie auf **OK**.

- Die Anwendung wird in die Firewall-Richtlinie aufgenommen und als **vertrauenswürdig** gekennzeichnet.
- Die Prüfsumme der Anwendung wird in die Liste der zulässigen Prüfsummen aufgenommen.

7.2.2.3.3 Entfernen einer Anwendung aus der Firewall-Richtlinie

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So können Sie eine Anwendung aus der Firewall-Richtlinie entfernen:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
4. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
5. Klicken Sie auf die Registerkarte **Anwendungen**.
6. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf **Entfernen**.

7.2.2.3.4 Zulassen einer Anwendung

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So lassen Sie eine Anwendung auf einer Computergruppe zu:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
4. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
5. Klicken Sie auf die Registerkarte **Anwendungen**.

   Wenn sich die Anwendung nicht in der Liste befindet, befolgen Sie die Anweisungen unter *Aufnahme einer Anwendung in eine Firewall-Richtlinie* (Seite 126), um sie hinzuzufügen.

6. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf **Vertrauen**.

- Die Anwendung wird in die Firewall-Richtlinie aufgenommen und als **vertrauenswürdig** gekennzeichnet.
- Die Prüfsumme der Anwendung wird in die Liste der zulässigen Prüfsummen aufgenommen.

Vertrauenswürdige Anwendungen erhalten uneingeschränkten Vollzugriff auf das Netzwerk und das Internet. Über *Anwendungsregeln* können Sie Bedingungen für die Ausführung der Anwendung festlegen und somit die Sicherheit erhöhen.

- *Erstellen einer Anwendungsregel* (Seite 141)
- *Übernahme vordefinierter Anwendungsregeln* (Seite 143)

7.2.2.3.5 Zulassen von Anwendungen über die Ereignisanzeige der Firewall

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wenn die Firewall auf einem Netzwerkcomputer eine unbekannte Anwendung meldet oder sperrt, wird in der Firewall-Ereignisanzeige ein entsprechendes Ereignis angezeigt. In diesem Abschnitt erfahren Sie, wie eine Anwendung aus der Firewall-Ereignisanzeige zugelassen wird und die neue Regel auf die ausgewählten Firewall-Richtlinien übertragen wird.

So finden Sie gemeldete und/oder gesperrte Anwendungen in der Firewall-Ereignisanzeige und lassen sie zu oder erstellen neue Regeln für sie:

1. Klicken Sie im Menü **Ereignisse** auf **Firewall-Ereignisse**.
2. Wählen Sie im Dialogfeld **Firewall – Ereignisanzeige** den Eintrag für die Anwendung aus, die als vertrauenswürdig eingestuft bzw. für die eine Regel erstellt werden soll, und klicken Sie auf **Regel erstellen**.
3. Wählen Sie im Dialogfeld aus, ob Sie die Anwendung zulassen möchten oder eine Regel dafür erstellen möchten.
4. Wählen Sie aus der Liste der Firewall-Richtlinien die Richtlinien aus, die Sie in die Regel aufnehmen möchten. Klicken Sie zur Übernahme der Regel für alle Richtlinien auf **Alles markieren** und klicken Sie anschließend auf **OK**.

- Wenn Sie Prüfsummen verwenden, müssen Sie die Prüfsumme der Anwendung unter Umständen in die Liste der erlaubten Prüfsummen aufnehmen. Mehr dazu erfahren Sie unter *Hinzufügen einer Anwendungsprüfsumme* (Seite 131).
- Mit den erweiterten Firewall-Richtlinienkonfigurationseinstellungen können Sie auch eine Anwendung als vertrauenswürdig einstufen und in die Firewall-Richtlinie aufnehmen. Mehr dazu erfahren Sie unter *Erstellen einer Anwendungsregel aus einer Firewall-Richtlinie* (Seite 142).

7.2.2.3.6 Sperren einer Anwendung

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So sperren Sie eine Anwendung auf einer Computergruppe:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
4. Klicken Sie im Bereich **Konfigurationen** neben dem zu konfigurierenden Standort auf **Konfigurieren**.
5. Klicken Sie auf die Registerkarte **Anwendungen**.

   Wenn sich die Anwendung nicht in der Liste befindet, befolgen Sie die Anweisungen unter *Aufnahme einer Anwendung in eine Firewall-Richtlinie* (Seite 126), um sie hinzuzufügen.
6. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf **Sperren**.

7.2.2.3.7 Zulassen versteckter Prozesse

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Eine Anwendung kann im Hintergrund einen anderen Prozess starten, der für sie auf das Netzwerk zugreift.

Malware kann auf diese Weise Firewalls umgehen: Zum Zugriff auf das Netzwerk wird eine vertrauenswürdige Anwendung und nicht die Malware selbst gestartet.

So erlauben Sie Anwendungen den Start versteckter Prozesse:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Prozesse**.

5. Klicken Sie im oberen Bereich auf **Hinzufügen**.

   Das Dialogfenster **Firewall-Richtlinie – Anwendung hinzufügen** wird angezeigt.

6. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Anwendungsereignisse angezeigt werden sollen.

   Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt Ihren eigenen Zeitraum bestimmen.

7. Wenn Sie Anwendungsereignisse eines bestimmten Typs aufrufen möchten, wählen Sie den gewünschten Typ im Dropdown-Menü **Ereignistyp** aus.
8. Wenn Sie Anwendungsereignisse für eine bestimmte Datei aufrufen möchten, geben Sie in das Feld **Dateiname** den entsprechenden Namen ein.

   Wenn Sie keine spezifischen Angaben machen, werden Anwendungsereignisse für alle Dateien angezeigt.

   Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.

9. Klicken Sie zur Anzeige einer Anwendungsereignisliste auf **Suche**.
10. Wählen Sie ein Anwendungsereignis aus der Liste und klicken Sie auf **OK**.

Im interaktiven Modus kann die Firewall Lerndialoge auf dem Endpoint anzeigen, wenn neue Startprogramme erkannt werden. Mehr dazu erfahren Sie unter *Aktivieren des interaktiven Modus* (Seite 124).

7.2.2.3.8 Zulassen von Raw-Sockets

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Einige Anwendungen können den Netzwerkzugriff über Raw-Sockets herstellen, wodurch sie die im Netzwerk gesendeten Daten beeinflussen können.

Schadprogramme können Raw-Sockets ausnutzen, indem sie deren IP-Adressen duplizieren oder korrumpierte Meldungen senden.

So lassen Sie den Zugriff über Raw-Sockets zu:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Prozesse**.

5. Klicken Sie im oberen Bereich auf **Hinzufügen**.

   Das Dialogfenster **Firewall-Richtlinie – Anwendung hinzufügen** wird angezeigt.

6. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Anwendungsereignisse angezeigt werden sollen.

   Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt Ihren eigenen Zeitraum bestimmen.

7. Wenn Sie Anwendungsereignisse eines bestimmten Typs aufrufen möchten, wählen Sie den gewünschten Typ im Dropdown-Menü **Ereignistyp** aus.
8. Wenn Sie Anwendungsereignisse für eine bestimmte Datei aufrufen möchten, geben Sie in das Feld **Dateiname** den entsprechenden Namen ein.

   Wenn Sie keine spezifischen Angaben machen, werden Anwendungsereignisse für alle Dateien angezeigt.

   Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.

9. Klicken Sie zur Anzeige einer Anwendungsereignisliste auf **Suche**.
10. Wählen Sie ein Anwendungsereignis aus der Liste und klicken Sie auf **OK**.

Im interaktiven Modus kann die Firewall Lerndialoge auf dem Endpoint anzeigen, wenn neue Raw-Sockets erkannt werden. Mehr dazu erfahren Sie unter *Aktivieren des interaktiven Modus* (Seite 124).

7.2.2.3.9 Hinzufügen einer Anwendungsprüfsumme

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Jede Version einer Anwendung umfasst eine andere Prüfsumme. Mit Hilfe der Prüfsumme kann die Firewall entscheiden, ob eine Anwendung zugelassen oder gesperrt werden soll.

Standardmäßig prüft die Firewall die Prüfsumme aller laufenden Prozesse. Wenn die Prüfsumme unbekannt ist oder sich geändert hat, wird sie von der Firewall blockiert.

So fügen Sie eine neue Prüfsumme hinzu:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie auf die Registerkarte **Prüfsummen**.
4. Klicken Sie auf **Hinzufügen**.

   Das Dialogfenster **Firewall-Richtlinie – Anwendungsprüfsumme hinzufügen** wird angezeigt.

5. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Anwendungsereignisse angezeigt werden sollen.

   Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt Ihren eigenen Zeitraum bestimmen.

6. Klicken Sie im Feld **Ereignistyp** auf den Dropdown-Pfeil und geben Sie an, ob eine Prüfsumme für geänderte oder neue Anwendungen hinzugefügt werden soll.
7. Wenn Sie Anwendungsereignisse für eine bestimmte Datei aufrufen möchten, geben Sie in das Feld **Dateiname** den entsprechenden Namen ein.

   Wenn Sie keine spezifischen Angaben machen, werden Anwendungsereignisse für alle Dateien angezeigt.

   Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.

8. Klicken Sie zur Anzeige einer Anwendungsereignisliste auf **Suche**.
9. Wählen Sie das Anwendungsereignis aus, für das Sie eine Prüfsumme hinzufügen möchten, und klicken Sie auf **OK**.

Die Anwendungsprüfsumme wird der Liste der zugelassenen Prüfsummen im Dialogfeld **Firewall-Richtlinie** hinzugefügt.

Im interaktiven Modus kann die Firewall Lerndialoge auf dem Endpoint anzeigen, wenn neue oder geänderte Anwendungen erkannt werden. Mehr dazu erfahren Sie unter *Aktivieren des interaktiven Modus* (Seite 124).

7.2.2.3.10 Aktivieren/Deaktivieren des Sperrens modifizierter Prozesse

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Unter Umständen versuchen Malware-Autoren die Firewall zu umgehen, indem ein Prozess im Speicher modifiziert wird, der von einem vertrauenswürdigen Programm eingeleitet wurde. Anschließend wird versucht, über den modifizierten Prozess Zugriff zum Netzwerk zu erlangen.

Sie können die Firewall zum Erkennen und Sperren von modifizierten Prozessen im Speicher konfigurieren.

Verfahren Sie zum Aktivieren/Deaktivieren des Sperrens modifizierter Prozesse wie folgt:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.

4. Deaktivieren Sie auf der Registerkarte **Allgemein** im Bereich **Sperren** die Option **Prozesse sperren, wenn Speicher durch andere Anwendung geändert wird**, um das Sperren modifizierter Prozesse zu deaktivieren.

   Wenn Sie das Sperren modifizierter Prozesse wieder aktivieren möchten, wählen Sie das Kontrollkästchen aus.

Wenn die Firewall erkennt, dass ein Prozess im Speicher geändert, werden Regeln hinzugefügt, die verhindern, dass der modifizierte Prozess auf das Netzwerk zugreift.

Hinweise

- Wir raten davon ab, das Sperren modifizierter Prozesse über einen längeren Zeitraum zu deaktivieren. Die Deaktivierung sollte sich auf den Bedarfsfall beschränken.
- Das Sperren modifizierter Prozesse wird auf 64-Bit-Versionen von Windows nicht unterstützt.
- Nur der modifizierte Prozess selbst kann gesperrt werden. Dem modifizierten Programm wird der Netzwerkzugriff jedoch nicht verweigert.

7.2.2.3.11 Filtern von ICMP-Meldungen

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

ICMP-Meldungen (Internet Control Message Protocol) ermöglichen Computern im Netzwerk die Freigabe von Fehler- und Statusinformationen. Sie können bestimmte Typen eingehender oder ausgehender ICMP-Meldungen zulassen oder sperren.

Die Filterung von ICMP-Meldungen empfiehlt sich lediglich, wenn Sie mit Netzwerkprotokollen vertraut sind. Im Abschnitt *Erläuterung der ICMP-Meldungen* (Seite 133) werden die ICMP-Meldungstypen beschrieben.

So filtern Sie ICMP-Meldungen:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Wählen Sie auf der Registerkarte **ICMP** die Option **Eingehend** oder **Ausgehend**, um eingehende bzw. ausgehende Meldungen des angegebenen Typs zuzulassen.

7.2.2.3.12 Erläuterung der ICMP-Meldungen

Echo-Anforderung, Echo-Antwort	Meldung zum Testen von Verfügbarkeit und Status des Ziels. Ein Host sendet eine **Echo-Anfrage** und wartet auf

	eine **Echo-Antwort**. Dies erfolgt in der Regel über den **ping**-Befehl.
Ziel nicht erreichbar, Echo-Antwort	Meldung eines Routers, der ein IP-Datagramm nicht abliefern kann. Ein Datagramm ist eine Dateneinheit oder ein Paket, die/das in einem TCP-/IP-Netzwerk übertragen wird.
Quelldrosselung	Meldung eines Hosts oder Routers, wenn Daten zu schnell eingehen und somit nicht verarbeitet werden können. Die Meldung ist als Aufforderung zur Verringerung der Datagramm-Übertragungsrate durch die Quelle zu verstehen.
Umleitung	Meldung eines Routers bei Empfang eines an einen anderen Router gerichteten Datagramms. Die Meldung umfasst die Adresse, an die Datagramme von der Quelle künftig gesendet werden sollen. Sie dient der Optimierung des Routings von Datenfluss im Netzwerk.
Router-Ankündigung, Router-Anfrage	Die Meldung macht Hosts auf Router aufmerksam. Router versenden regelmäßig ihre IP-Adressen über **Router-Ankündigungsmeldungen**. Mitunter fordern Hosts mittels **Router-Anfragen** Router-Adressen an. Die Antwort durch den Router erfolgt über **Router-Ankündigungen**.
Datagramm-Zeitüberschreitung	Meldung eines Routers, wenn ein Datagramm die maximale Routeranzahl erreicht hat.
Datagramm-Parameterproblem	Meldung eines Routers, wenn bei der Übertragung eines Datagramms ein Problem auftritt und die Verarbeitung nicht abgeschlossen werden kann. Solche Probleme werden beispielsweise durch ungültige Datagramm-Header verursacht.
Zeitstempel-Anforderung, Zeitstempel-Antwort	Dient der zeitlichen Synchronisierung von Hosts und der Schätzung der Transitzeit.
Informations-Anforderung, Informations-Antwort	Veraltet. Die Meldungen wurden zur Bestimmung der Internetwork-Adressen von Hosts eingesetzt, gelten jetzt aber als veraltet und sollten nicht mehr verwendet werden.
Adressmasken-Anforderung, Adressmasken-Antwort	Meldung zur Ermittlung der Subnetz-Maske (d.h. der Adressabschnitte, die das Netzwerk definieren). Ein Host sendet eine **Adressmasken-Anforderung** an einen Router und empfängt eine **Adressmasken-Antwort**.

7.2.2.4 Firewall-Regeln

7.2.2.4.1 Allgemeine Informationen

Globale Regeln

Globale Regeln gelten für die gesamte Netzwerkkommunikation sowie für Anwendungen, für die Anwendungsregeln erstellt wurden.

Anwendungsregeln

Einer Anwendung kann eine oder mehrere Regeln zugewiesen werden. Sie können die vordefinierten Regeln von Sophos verwenden oder benutzerdefinierte Regeln erstellen und so den Zugriff auf eine Anwendung ganz an die Bedürfnisse in Ihrem Unternehmen anpassen.

7.2.2.4.2 Reihenfolge der Regeln

Für Raw-Socket-Verbindungen werden nur die globalen Regeln abgerufen.

In Abhängigkeit davon, ob die Verbindung zu einer Netzwerkadresse in der Registerkarte **LAN** besteht, werden bei Verbindungen *ohne* Raw-Sockets werden diverse Regeln geprüft.

Wenn die Netzwerkadresse nicht in der Registerkarte **LAN** aufgeführt wird, werden die folgenden Regeln geprüft:

- Wenn die Adresse als **Zuverlässig** ausgewiesen wird, wird der gesamte über diese Verbindung laufende Datenfluss ohne weitere Prüfungen zugelassen.
- Wenn die Adresse als **NetBIOS** ausgewiesen wurde, wird Datei- und Druckerfreigabe auf allen Verbindungen zugelassen, die die folgenden Voraussetzungen erfüllt:

Verbindung	Port	Reichweite
TCP	Remote	137-139 oder 445
TCP	Lokal	137-139 oder 445
UDP	Remote	137 oder 138
UDP	Lokal	137 oder 138

Wenn sich die Netzwerkadresse *nicht* in der Registerkarte **LAN** befindet, werden andere Firewall-Regeln in der folgenden Reihenfolge geprüft:

1. **NetBIOS**-Datenfluss, der nicht auf der Registerkarte **LAN** zugelassen wird, wird über die Option **Datei- und Druckerfreigabe für andere Netzwerke sperren** geregelt:
   - Wenn die Option aktiviert ist, wird der Datenfluss gesperrt.
   - Wenn die Option nicht aktiviert ist, regeln die restlichen Regeln den Datenfluss.
2. Die globalen Richtlinien hoher Priorität werden in der aufgelisteten Reihenfolge abgerufen.
3. Wenn der Verbindung noch keine Regel zugewiesen wurde, werden Anwendungsregeln abgerufen.
4. Wenn die Verbindung immer noch nicht erfasst wurde, werden die globalen Regeln normaler Priorität in der festgelegten Reihenfolge abgerufen.
5. Wenn keine Regeln für die Verbindung abgerufen werden konnten:
   - Im Modus **Datenfluss ohne passende Regel zulassen** wird der (ausgehende) Datenfluss zugelassen.

- Im Modus **Datenfluss ohne passende Regel sperren** wird der Datenfluss gesperrt.
- Im Modus **Interaktiv** wird der Benutzer gefragt, wie er mit der Verbindung verfahren möchte.

Hinweis: Wenn Sie den Arbeitsmodus nicht geändert haben, befindet sich die Firewall im Modus **Standardmäßig sperren**.

7.2.2.4.3 Lokale Netzwerkerkennung

Sie können den Firewall-Regeln für diesen Computer ein lokales Netzwerk zuweisen.

Die Firewall ermittelt das lokale Netzwerk des Computers beim Starten und stellt bei der Ausführung ggf. Änderungen fest. Bei Änderungen aktualisiert die Firewall die Regeln des lokalen Netzwerks mit dem neuen Adressbereich des lokalen Netzwerks.

Vorsicht: Bei lokalen Netzwerkregeln in sekundären Konfigurationen ist Vorsicht geboten. Laptops, die außerhalb des Unternehmens eingesetzt werden, stellen unter Umständen eine Verbindung zu einem unbekannten lokalen Netzwerk her. Wenn dies der Fall ist, wird aufgrund der Firewallregeln der sekundären Konfiguration, bei denen die Adresse das lokale Netzwerk ist, unter Umständen der gesamte unbekannte Datenverkehr zugelassen.

7.2.2.4.4 Globale Regeln

7.2.2.4.4.1 Standardeinstellungen globaler Regeln

In diesem Abschnitt werden Bedingungen und Maßnahmen zu den standardmäßigen globalen Regeln erläutert. Es empfiehlt sich, diese Einstellungen beim Erstellen einer neuen standardmäßigen globalen Regel zu beachten.

DNS-Auflösung (TCP) zulassen

- Protokoll: TCP
- Richtung: Ausgehend
- Remote-Port: DOMÄNE
- Maßnahme: Zulassen

DNS-Auflösung (UDP) zulassen

- Protokoll: UDP
- Richtung: Ausgehend
- Remote-Port: DNS
- Maßnahme: Stateful Inspection zulassen

Ausgehendes DHCP zulassen

- Protokoll: UDP
- Lokaler Port: BOOTPS,BOOTPC,546,547
- Maßnahme: Zulassen

Eingehende Identifizierung zulassen

- Protokoll: TCP

- Richtung: Eingehend
- Lokaler Port: AUTH
- Maßnahme: Zulassen

Loopback zulassen

- Protokoll: TCP
- Richtung: Eingehend
- Lokaler Port: 127.0.0.0 (255.255.255.0)
- Maßnahme: Zulassen

GRE-Protokoll zulassen

- Protokoll: TCP
- Protokolltyp: Ausgehend
- Maßnahme: Zulassen

PPTP-Control-Verbindung zulassen

- Protokoll: TCP
- Richtung: Ausgehend
- Remote-Port: PPTP
- Lokaler Port: 1024-65535
- Maßnahme: Zulassen

RPC-Call (TCP) sperren

- Protokoll: TCP
- Richtung: Eingehend
- Lokaler Port: DCOM
- Maßnahme: Sperren

RPC-Call (UDP) sperren

- Protokoll: UDP
- Lokaler Port: 135
- Maßnahme: Sperren

Server Message Block-Protokoll (UDP) sperren

- Protokoll: TCP
- Richtung: Eingehend
- Lokaler Port: MICROSOFT_DS
- Maßnahme: Sperren

Server Message Protokoll (UDP) sperren

- Protokoll: TCP
- Lokaler Port: 445
- Maßnahme: Sperren

Localhost-Verbindung (UDP) zulassen

- Protokoll: UDP
- Remote-Host: 255.255.255.255 (0.0.0.0)
- Lokaler Host: 255.255.255.255 (0.0.0.0)
- Der lokale Port ist dem Remote-Port dabei gleich: True
- Maßnahme: Zulassen

7.2.2.4.4.2 *Erstellen einer globalen Regel*

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wichtig: Das Erstellen globaler Regeln empfiehlt sich lediglich, wenn Sie sich mit Netzwerkprotokollen auskennen.

Globale Regeln gelten für alle Datenbewegungen im Netzwerk und für Anwendungen, denen noch keine Regel zugewiesen wurde.

So erstellen Sie eine globale Regel:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Globale Regel**.
5. Klicken Sie auf **Hinzufügen**.
6. Geben Sie unter **Regelname** den gewünschten Regelnamen ein.

   Der Regelname darf in einer Regelliste nicht mehrfach verwendet werden. Alle globalen Regeln müssen einen eindeutigen Namen haben.
7. Wenn die Regel vor Anwendungsregeln oder anderen Regeln normaler Priorität greifen soll, wählen Sie die Option **Regel mit hoher Priorität**.

   Weitere Informationen zur Regelpriorität finden Sie unter *Reihenfolge der Regeln* (Seite 135).

8. Wählen Sie im Bereich **Ereignisse, für die die Regel zutreffen soll** die Bedingungen aus, die eine Verbindung erfüllen muss, damit die Regel greift.
9. Wählen Sie im Bereich **Maßnahmen, die die Regel ergreifen soll Zulassen** oder **Sperren** aus.
10. Führen Sie einen der folgenden Schritte aus:
    - Wählen Sie die Option **Gleichzeitige Verbindungen** aus, damit weitere Verbindungen von und an die gleiche Remote-Adresse möglich sind, auch wenn die ursprüngliche Verbindung besteht.

      Hinweis: Die Option beschränkt sich auf TCP-Regeln, die standardmäßig statusbehaftet sind.
    - Bei Auswahl der Option **Stateful Inspection** basieren die Antworten des Remote-Computers auf der ersten Verbindung.
11. Klicken Sie im Bereich **Regelbeschreibung** auf einen unterstrichenen Wert. Wenn Sie beispielsweise auf den Link **TCP** klicken, wird das Dialogfeld **Protokoll wählen** geöffnet.

7.2.2.4.4.3 *Ändern einer globalen Regel*

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wichtig: Das Ändern globaler Regeln empfiehlt sich lediglich, wenn Sie sich mit Netzwerkprotokollen auskennen.

So ändern Sie eine globale Regel:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Globale Regel**.
5. Wählen Sie die gewünschte Regel aus der **Regelliste** aus.
6. Klicken Sie auf **Bearbeiten**.

   Nähere Informationen zu den Einstellungen globaler Regeln können Sie dem Abschnitt *Standardeinstellungen globaler Regeln* (Seite 136) entnehmen.

7.2.2.4.4.4 *Kopieren einer globalen Regel*

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.

- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So kopieren Sie eine globale Regel und nehmen sie in die Regelliste auf:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Globale Regel**.
5. Wählen Sie die gewünschte Regel aus der **Regelliste** aus.
6. Klicken Sie auf **Kopieren**.

7.2.2.4.4.5 *Löschen einer globalen Regel*

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Globale Regel**.
5. Wählen Sie die gewünschte Regel aus der **Regelliste** aus.
6. Klicken Sie auf **Entfernen**.

7.2.2.4.4.6 *Ändern der Priorität von globalen Regeln*

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Globale Regeln werden in der Reihenfolge angewandt, in der sie in der Regelliste aufgeführt werden (von oben nach unten).

So können Sie die Priorität von globalen Regeln ändern:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Globale Regel**.
5. Klicken Sie in der **Regelliste** auf die Regel, die Sie nach oben oder unter verschieben möchten.
6. Klicken Sie auf **Nach oben** oder **Nach unten**.

7.2.2.4.5 Anwendungsregeln

7.2.2.4.5.1 Erstellen einer Anwendungsregel

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So erstellen Sie eine Anwendungsregel, um den Zugriff auf eine bestimmte Anwendung an die Bedürfnisse in Ihrem Unternehmen anzupassen:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Anwendungen**.
5. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf den Pfeil neben der Option **Regel** .
6. Klicken Sie im Dialogfeld **Anwendungsregeln** auf **Hinzufügen**.
7. Geben Sie unter **Regelname** den gewünschten Regelnamen ein.

   Der Regelname darf in einer Regelliste nicht mehrfach verwendet werden. Jedoch können zwei Anwendungen gleichnamige Regeln zugewiesen werden.
8. Wählen Sie im Bereich **Ereignisse, für die die Regel zutreffen soll** die Bedingungen aus, die eine Verbindung erfüllen muss, damit die Regel greift.
9. Wählen Sie im Bereich **Maßnahmen, die die Regel ergreifen soll Zulassen** oder **Sperren** aus.
10. Bei Auswahl der Option **Stateful Inspection** basieren die Antworten des Remote-Computers auf der ersten Verbindung.
11. Klicken Sie im Bereich **Regelbeschreibung** auf einen unterstrichenen Wert. Wenn Sie beispielsweise auf den Link **TCP** klicken, wird das Dialogfeld **Protokoll wählen** geöffnet.

7.2.2.4.5.2 Erstellen einer Anwendungsregel aus einer Firewall-Richtlinie

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Mit den erweiterten Firewall-Richtlinieneinstellungen können Sie eine Anwendungsregel direkt aus einer Firewall-Richtlinie heraus erstellen.

So erstellen Sie eine Anwendungsregel aus einer Firewall-Richtlinie:

1. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
2. Klicken Sie auf der Startseite des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Fenster **Firewall-Richtlinie** neben dem Standort, für den die Firewall konfiguriert werden soll, auf **Konfigurieren**.
4. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie eine Anwendung zur Firewall-Richtlinie hinzufügen möchten, öffnen Sie die Registerkarte **Anwendungen** und klicken Sie auf **Hinzufügen**.
   - Wenn eine Anwendung versteckte Prozesse starten dürfen soll, öffnen Sie die Registerkarte **Prozesse** und klicken Sie im oberen Bereich auf **Hinzufügen**.
   - Wenn eine Anwendung über Rawsockets auf das Netzwerk zugreifen dürfen soll, öffnen Sie die Registerkarte **Prozesse** und klicken Sie im unteren Bereich auf **Hinzufügen**.

   Das Dialogfenster **Firewall-Richtlinie – Anwendung hinzufügen** wird angezeigt.
5. Wenn Sie eine Anwendung hinzufügen, wählen Sie im Feld **Ereignistyp**, ob Sie eine geänderte Anwendung, eine neue Anwendung oder eine Anwendung hinzufügen möchten, für die es in der Firewall-Richtlinie keine Anwendungsregel gibt.
6. Wählen Sie einen Eintrag für die Anwendung aus, die Sie hinzufügen möchten oder der das Starten versteckter Prozesse oder die Verwendung von Rawsockets gestattet werden soll. Klicken Sie auf **OK**.

   Die Anwendung wird zur Firewall-Richtlinie hinzugefügt.

Wenn Sie auf der Registerkarte **Anwendungen** eine Anwendung hinzugefügt haben, wird die Anwendung als vertrauenswürdig hinzugefügt. Sie können sie jetzt sperren oder eine benutzerdefinierte Regel dafür erstellen.

7.2.2.4.5.3 Bearbeiten einer Anwendungsregel

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Anwendungen**.
5. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf den Pfeil neben der Option **Regel** .
6. Klicken Sie im Dialogfeld **Anwendungsregeln** auf **Bearbeiten**.
7. Geben Sie unter **Regelname** den gewünschten Regelnamen ein.

   Der Regelname darf in einer Regelliste nicht mehrfach verwendet werden. Jedoch können zwei Anwendungen gleichnamige Regeln zugewiesen werden.
8. Wählen Sie im Bereich **Ereignisse, für die die Regel zutreffen soll** die Bedingungen aus, die eine Verbindung erfüllen muss, damit die Regel greift.
9. Wählen Sie im Bereich **Maßnahmen, die die Regel ergreifen soll Zulassen** oder **Sperren** aus.
10. Bei Auswahl der Option **Stateful Inspection** basieren die Antworten des Remote-Computers auf der ersten Verbindung.
11. Klicken Sie im Bereich **Regelbeschreibung** auf einen unterstrichenen Wert. Wenn Sie beispielsweise auf den Link **TCP** klicken, wird das Dialogfeld **Protokoll wählen** geöffnet.

7.2.2.4.5.4 *Übernahme vordefinierter Anwendungsregeln*

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Bei einer vordefinierten Regel handelt es sich um einen Satz von Anwendungsregeln, der von Sophos erstellt wurde. So fügen Sie einer Anwendung vordefinierte Regeln zur bestehenden Liste hinzu:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Anwendungen**.
5. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf den Pfeil neben der Option **Regel** .
6. Richten Sie den Mauszeiger auf **Regeln aus Voreinstellungen hinzufügen** und klicken Sie auf eine vordefinierte Regel.

7.2.2.4.5.5 Kopieren einer Anwendungsregel

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So kopieren Sie eine Anwendungsregel und nehmen sie in die Regelliste auf:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Anwendungen**.
5. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf den Pfeil neben der Option **Regel** .
6. Klicken Sie im Dialogfeld **Anwendungsregeln** auf **Kopieren**.

7.2.2.4.5.6 Löschen einer Anwendungsregel

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Anwendungen**.
5. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf den Pfeil neben der Option **Regel** .
6. Klicken Sie im Dialogfeld **Anwendungsregeln** auf **Entfernen**.

7.2.2.4.5.7 Ändern der Priorität von Anwendungsregeln

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.

- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Anwendungsregeln werden in der Reihenfolge angewandt, in der sie in der Regelliste aufgeführt werden (von oben nach unten).

So können Sie die Priorität von Anwendungsregeln ändern:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Anwendungen**.
5. Wählen Sie die Anwendung aus der Liste aus und klicken Sie anschließend auf den Pfeil neben der Option **Regel** .
6. Klicken Sie in der **Regelliste** auf die Regel, die Sie nach oben oder unter verschieben möchten.
7. Klicken Sie auf **Nach oben** oder **Nach unten**.

7.2.2.5 Standortspezifische Konfiguration

7.2.2.5.1 Allgemeine Informationen

Die standortspezifische Konfiguration ist eine Funktion von Sophos Client Firewall. Hierbei wird allen Netzwerkadpatern des Computers je nach aktuellem Standort des Netzwerkadapters eine Firewall-Konfiguration zugewiesen.

Die Funktion bietet sich an, wenn Sie ein Unternehmenslaptop besitzen und von zu Hause aus arbeiten. Sie verwenden zwei Netzwerkverbindungen gleichzeitig:

- Wenn Sie den Computer zu Unternehmenszwecken nutzen, stellen Sie eine Verbindung über einen VPN-Client und einen **virtuellen Netzwerkadpater** zum Unternehmensnetzwerk her.
- Für den Privatgebrauch stellen Sie über ein Netzwerkkabel und einen **physischen Netzwerkadapter** eine Verbindung zum Internet her.

In diesem Beispiel müssen Sie die Unternehmenskonfiguration auf die virtuelle Unternehmensverbindung und die (in der Regel strengere) Konfiguration für unternehmensfremde Zwecke auf die physische Verbindung anwenden.

Hinweis: Die Konfiguration für unternehmensfremde Zwecke muss genügend Regeln umfassen, damit die virtuelle Unternehmenskonfiguration hergestellt werden kann.

7.2.2.5.2 Einrichtung der standortspezifischen Konfiguration

1. Erstellen Sie ein Liste von Gateway-MAC-Adressen oder Domänennamen Ihrer Primärstandorte. Hierbei handelt es sich in der Regel um Ihre Unternehmensnetzwerke.
2. Erstellen Sie die Firewallkonfiguration für Ihre Primärstandorte. Die Konfiguration ist in der Regel weniger restriktiv.

3. Erstellen Sie eine sekundäre Firewallkonfiguration. In der Regel ist diese Konfiguration restriktiver.
4. Wählen Sie die gewünschte Konfiguration aus.

Je nach verwendeter Erkennungsmethode bezieht die Firewall die DNS- oder Gateway-Adressen für alle Netzwerkadapter der Computer und stimmt diese im Anschluss mit der Adressliste ab.

- Wenn eine Adresse in der Liste mit der Adresse eines Netzwerkadapters übereinstimmt, wird dem Adapter die Konfiguration des **Primärstandorts** zugewiesen.
- Wenn keine Adresse in der Liste mit der Adresse eines Netzwerkadapters übereinstimmt, wird dem Adapter die Konfiguration des **Sekundärstandorts** zugewiesen.

Wichtig: Die sekundäre Konfiguration wechselt vom **interaktiven** Modus in den Modus **Standardmäßig sperren**, wenn die beiden folgenden Bedingungen erfüllt sind:

- Beide Standorte sind aktiv.
- Die primäre Konfiguration ist *nicht* interaktiv.

7.2.2.5.3 Festlegen der primären Standorte

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Standorterkennung**.
5. Klicken Sie im Bereich **Erkennungsmethode** auf die Schaltfläche **Konfigurieren** neben der gewünschten Option:

Option	Beschreibung
DNS-Suche	Sie können eine Liste mit Domänennamen und erwarteten IP-Adressen erstellen, die Ihren primären Standorten entsprechen.
MAC-Adressenerkennung	Sie können eine Liste mit Gateway-MAC-Adressen erstellen, die Ihren primären Standorten entsprechen.

6. Befolgen Sie die Anweisungen auf dem Bildschirm.

7.2.2.5.4 Festlegen des sekundären Standorts

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Aktivieren Sie das Kontrollkästchen **Konfiguration für einen sekundären Standort**.

Konfigurieren Sie den sekundären Standort. Anweisungen hierzu finden Sie im Abschnitt *Konfigurieren der Firewall*.

Vorsicht: Bei lokalen Netzwerkregeln in sekundären Konfigurationen ist Vorsicht geboten. Laptops, die außerhalb des Unternehmens eingesetzt werden, stellen unter Umständen eine Verbindung zu einem unbekannten lokalen Netzwerk her. Wenn dies der Fall ist, wird aufgrund der Firewallregeln der sekundären Konfiguration, bei denen die Adresse das lokale Netzwerk ist, unter Umständen der gesamte unbekannte Datenverkehr zugelassen.

7.2.2.5.5 Auswahl einer Konfiguration

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf der Registerkarte **Allgemein** im Bereich **Standort** auf eine der folgenden Optionen:

Option	Beschreibung
Konfiguration des erkannten Standorts	Je nach Netzwerkverbindung weist die Firewall in Einklang mit den Erkennungseinstellungen der standortspezifischen Konfiguration immer die primäre oder die sekundäre Konfiguration zu (nähere Informationen hierzu finden Sie im Abschnitt *Einrichtung der standortspezifischen Konfiguration* (Seite 145)).
Konfiguration des primären Standorts	Die Firewall überträgt die primäre Konfiguration auf alle Netzwerkverbindungen.
Konfiguration des sekundären Standorts	Die Firewall überträgt die sekundäre Konfiguration auf alle Netzwerkverbindungen.

7.2.2.6 Firewall-Meldungen

7.2.2.6.1 Allgemeine Informationen

Standardmäßig meldet die Firewall auf dem Endpoint Änderungen, Ereignisse und Fehler an Enterprise Console.

Firewall-Status-Änderungen

Als Statusänderungen gelten:

- Wechsel des Arbeitsmodus
- Änderungen an der Softwareversion
- Änderungen mit Bezug auf das Zulassen von Datenfluss in der Firewall
- Änderungen mit Bezug auf die Richtlinienkonformität der Firewall

Im interaktiven Modus kann die Firewall-Konfiguration von der Richtlinie für Enterprise Console abweichen. Dies ist kein Zufall. In diesem Fall können Sie Alerts zu Abweichungen von der Richtlinie an Enterprise Console bei Änderungen an der Firewall-Konfiguration **deaktivieren**.

Weitere Informationen finden Sie unter *Aktivieren/Deaktivieren der Meldungen über lokale Änderungen* (Seite 148).

Firewall-Ereignisse

Ein *Ereignis* findet statt, wenn das Betriebssystem oder eine unbekannte Anwendung auf dem Computer versucht, über eine Netzwerkverbindung mit einem anderen Computer zu kommunizieren.

Sie können Ereignismeldungen an Enterprise Console deaktivieren.

Weitere Informationen finden Sie unter *Deaktivieren von Meldungen über unbekannte Datenbewegungen* (Seite 149).

7.2.2.6.2 Aktivieren/Deaktivieren der Meldungen über lokale Änderungen

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wenn die Firewall-Konfiguration von der Richtlinie abweicht, können Sie **Meldungen über lokale Änderungen deaktivieren**.

Wenn Sie die Meldungen über lokale Änderungen deaktivieren, sendet die Firewall nach Änderungen an globalen Regeln, Anwendungen, Prozessen oder Prüfsummen keine Alerts der Art „weicht von Richtlinie ab“ mehr an Enterprise Console. Eine Deaktivierung empfiehlt sich z.B. für den interaktiven Modus, da sich diese Einstellungen durch Lernregeln jederzeit anpassen lassen.

Wenn die Firewall-Konfiguration richtlinienkonform sein soll, sollten Sie **Meldungen über lokale Änderungen aktivieren**.

So deaktivieren Sie Meldungen über lokale Änderungen:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Allgemein**.
5. Wählen Sie im Bereich **Reports** eine der folgenden Funktionen aus:
   - Wenn lokale Änderungen gemeldet werden sollen, aktivieren Sie bitte das Kontrollkästchen **Lokal geänderte globale Regeln, Anwendungen, Prozesse und Prüfsummen an die Management-Konsole melden**.
   - Wenn lokale Änderungen nicht gemeldet werden sollen, deaktivieren Sie bitte das Kontrollkästchen **Lokal geänderte globale Regeln, Anwendungen, Prozesse und Prüfsummen an die Management-Konsole melden**.

7.2.2.6.3 Deaktivieren von Meldungen über unbekannte Datenbewegungen

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können festlegen, dass die Firewall auf den Endpoints unbekannte Datenbewegungen nicht an Enterprise Console meldet. Datenbewegungen, die keinen Regeln entsprechen, werden von der Firewall als „unbekannt“ eingestuft.

So können Sie festlegen, dass die Firewall auf den Endpoints unbekannte Datenbewegungen nicht an Enterprise Console meldet:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Allgemein**.
5. Aktivieren Sie im Bereich **Sperren** das Kontrollkästchen **Anwendungen anhand von Prüfsummen authentifizieren**.
6. Deaktivieren Sie unter **Reports** das Kontrollkästchen **Neue und geänderte Anwendungen an die Management-Konsole melden**.

7.2.2.6.4 Deaktivieren von Firewall-Fehlermeldungen

Wichtig: Wir raten davon ab, Firewall-Fehlermeldungen über einen längeren Zeitraum zu deaktivieren. Die Deaktivierung sollte sich auf den Bedarfsfall beschränken.

So verhindern Sie, dass die Firewall auf dem Endpoint Fehler an Enterprise Console meldet:

1. Doppelklicken Sie auf die zu ändernde Firewall-Richtlinie.
2. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
3. Klicken Sie im Bereich **Konfigurationen** neben dem Standort, für den Sie die Firewall konfigurieren möchten, auf **Konfigurieren**.
4. Klicken Sie auf die Registerkarte **Allgemein**.
5. Deaktivieren Sie unter **Reports** das Kontrollkästchen **Fehler an die Management-Konsole melden**.

7.2.2.7 Importieren/Exportieren der Firewall-Konfiguration

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Firewall-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Firewall** verfügen.

- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können allgemeine Firewall-Einstellungen und -Regeln als Konfigurationsdatei (*.conf) importieren oder exportieren. Diese Funktion umfasst folgende Optionen:

- Sichern und Wiederherstellen der Firewall-Konfiguration.
- Importieren von auf einem Computer erstellten Anwendungsregeln und Erstellen einer Richtlinie für andere Computer mit den gleichen Anwendungen auf der Basis der Anwendungsregeln.
- Kombination der Konfiguration unterschiedlicher Computer zur Erstellung einer für eine oder mehrere Computergruppen gültige Richtlinie.

Verfahren Sie zum Importieren/Exportieren der Firewall-Konfiguration wie folgt:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Feld **Richtlinien** auf **Firewall** und doppelklicken Sie anschließend auf die Richtlinie, die Sie importieren/exportieren möchten.
3. Klicken Sie auf der **Startseite** des **Firewall-Richtlinienassistenten** auf **Erweiterte Einstellungen**.
4. Klicken Sie im Dialogfeld **Firewall-Richtlinie** auf der Registerkarte **Allgemein** unter **Konfiguration verwalten** auf **Importieren** bzw. **Exportieren**.

7.3 Konfigurieren der NAC-Richtlinie

7.3.1 NAC

Sie können Network Access Control (NAC) so konfigurieren, dass Computer nur auf das Netzwerk zugreifen können, wenn sie die von Ihnen bestimmten Voraussetzungen erfüllen. Standardmäßig wird Computern der Netzwerkzugriff gewährt.

Enterprise Console schützt das Netzwerk in Kombination mit NAC Manager. Sie müssen Folgendes installiert haben:

- NAC Manager. Dieser Server wird unabhängig von Enterprise Console installiert.
- NAC Agent. NAC Manager wird auf Ihren Computern im Netzwerk installiert, um die Kommunikation mit NAC Manager zu gewährleisten. Den Agenten können Sie über den **Assistenten zum Schutz von Computern** installieren. Mehr dazu erfahren Sie unter *Automatisches Schützen von Computern* (Seite 51).

Hier wird davon ausgegangen, dass Sie beide Komponenten installiert haben.

Hinweis: Bei rollenbasierter Verwaltung müssen Sie zum Bearbeiten einer NAC-Richtlinie über die Berechtigung **Richtlinieneinstellung – NAC** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

7.3.2 Einrichten der NAC-Server-URL

Wenn Sie mit NAC arbeiten möchten, müssen Sie die URL des NAC-Servers (d.h. des Computers, auf dem NAC Manager installiert wurde) in Enterprise Console angeben. Dies erfüllt folgende Zwecke:

- Ihre Computer können mit NAC Manager kommunizieren und die richtige NAC-Richtlinie empfangen.
- In NAC Manager können Sie NAC-Richtlinien konfigurieren.

Enterprise Console versucht nach der Erstinstallation, den NAC-Server zu finden und sich damit zu verbinden. Wenn dies nicht gelingt oder sich der Standort des NAC-Servers geändert hat, müssen Sie die URL ggf. selbst angeben.

So geben Sie die URL ein:

1. Wählen Sie im Menü **Extras** die Option **NAC-URL konfigurieren**.
2. Geben Sie im Dialogfeld **URL des Sophos NAC-Servers** die URL des NAC-Servers ein (z.B. http://server).

   Hinweis: Wenn Sophos NAC auf mehr als einem Server installiert ist, geben Sie statt der Adresse des Computers mit der Datenbank die Adresse des Computers ein, auf dem die Anwendung läuft.

3. Um zu testen, ob Enterprise Console eine Verbindung über die angegebene URL mit dem NAC-Server herstellen kann, klicken Sie auf **Test**.

7.3.3 Starten von NAC Manager

NAC Manager ist das Programm, mit dem Sie die NAC-Richtlinien ändern können.

So starten Sie NAC Manager:

1. Klicken Sie in der Symbolleiste auf **NAC**.

   Sie können jedoch auch im Menü **Extras** die Option **NAC verwalten** wählen.

   Hinweis: Wenn die URL des NAC-Servers noch nicht erkannt oder eingegeben wurde, werden Sie dazu jetzt aufgefordert.

2. Geben Sie zur Anmeldung Ihre Benutzerdaten für Sophos NAC ein, die Sie von Ihrem Sophos NAC Administrator erhalten haben.

Wie dieses Programm genau funktioniert, erfahren Sie in der Hilfe zu Sophos NAC Manager oder der *Sophos NAC für Endpoint Security and Control NAC Manager-Anleitung* .

7.3.4 NAC-Voreinstellungen

Als Voreinstellung wird die **Standard**-NAC-Richtlinie auf Computer mit Sophos NAC übertragen. Wenn Sie den „Richtlinien-Modus“ nicht geändert haben, gilt Folgendes:

- Die Computer haben Netzwerkzugriff.

- NAC wird im Modus „Report Only“ ausgeführt.

Nähere Informationen zu **verwalteten** und **unverwalteten** Richtlinien finden Sie im Abschnitt *Voreingestellte NAC-Richtlinien* (Seite 152)

7.3.5 Voreingestellte NAC-Richtlinien

Es gibt drei voreingestellte Richtlinien. Im Abschnitt *Ändern einer NAC-Richtlinie* (Seite 152) erfahren Sie, wie Sie die Einstellungen dieser Richtlinien ändern können.

Default

Diese Richtlinie wird standardmäßig auf Computer übertragen, auf denen Sophos NAC installiert ist. Wenn Sie die Einstellungen dieser Richtlinie nicht geändert haben, sind alle Computer mit Netzwerkzugriffsrechten ausgestattet. NAC wird im Modus „Report Only“ ausgeführt.

Managed

Diese Richtlinie bietet sich für Computer mit NAC an, die von Enterprise Console verwaltet werden. Die Voreinstellungen entsprechen der Standardrichtlinie.

Nicht verwaltet

Diese Richtlinie kann für Computer an einem Remote-Standort verwendet werden, die nicht von Enterprise Console verwaltet werden und nicht über Sophos NAC verfügen. Temporäre Netzwerkbenutzer können zur Verbindungsherstellung mit einer Website aufgefordert werden, die den entsprechenden Remote-Computer über einen Web-Agenten mit der Richtlinie vergleicht, bevor er den Zugriff auf das Unternehmensnetzwerk freigibt.

7.3.6 Ändern einer NAC-Richtlinie

Bei rollenbasierter Verwaltung müssen Sie zum Bearbeiten einer NAC-Richtlinie über die Berechtigung **Richtlinieneinstellung – NAC** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können die Einstellungen der voreingestellten NAC-Richtlinien an Ihre Bedürfnisse anpassen. Sie können die Richtlinien in NAC Manager bearbeiten, um den Richtlinienmodus, die Profile der Richtlinie oder die der Richtlinie zugewiesenen Network Access Templates zu ändern.

So können Sie eine NAC-Richtlinie ändern:

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **NAC**. Doppelklicken Sie auf die Richtlinie, die Sie konfigurieren möchten.

   NAC Manager wird gestartet.

2. Melden Sie sich mit Ihren Benutzerdaten an.
3. Passen Sie auf der Richtlinienseite die gewünschten Optionen an.

Näheres zum Updaten vorhandener Richtlinie erfahren Sie in der *Konfigurationsanleitung zu Sophos NAC Manager*.

7.4 Konfigurieren der Application Control-Richtlinie

7.4.1 Was ist Application Control?

Mit Enterprise Console können Sie Controlled Applications erkennen und sperren, d.h. legitime Anwendungen, die zwar kein Sicherheitsrisiko darstellen, die aber für Ihre Unternehmensumgebung ungeeignet sind. Zu solchen Anwendungen gehören Instant Messaging (IM) Clients, Voice Over Internet Protocol (VoIP) Clients, Digital Imaging Software, Medienplayer, Browser Plug-Ins usw.

Hinweis: Die Option beschränkt sich auf Sophos Endpoint Security and Control für Windows 2000 und aufwärts.

Anwendungen können für verschiedene Computergruppen völlig flexibel gesperrt oder zugelassen werden. Beispielsweise kann VoIP für Computer im Unternehmen ausgeschaltet, für Remote-Computer aber zugelassen werden.

Die Liste der Controlled Applications wird von Sophos zur Verfügung gestellt und regelmäßig aktualisiert. Sie können keine neuen Anwendungen in die Liste aufnehmen. Auf Wunsch können Sie jedoch bei Sophos die Aufnahme einer Anwendung, die im Netzwerk kontrolliert werden soll, in die Liste beantragen. Nähere Informationen finden Sie im Support-Artikel 35330 (*http://www.sophos.de/support/knowledgebase/article/35330.html*).

In diesem Abschnitt wird beschrieben, wie Sie die Anwendungen auswählen, die Sie in ihrem Netzwerk kontrollieren möchten und Scans für Controlled Applications einrichten.

Hinweis: Bei rollenbasierter Verwaltung:

- Zur Konfiguration einer Application Control-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellungen – Application Control** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 17) entnehmen.

Application Control-Ereignisse

Application Control-Ereignisse (z.B. eine erkannte Controlled Application im Netzwerk) werden im Application Control-Ereignisprotokoll verzeichnet und können in Enterprise Console aufgerufen werden. Mehr dazu erfahren Sie unter *Anzeigen von Application Control-Ereignissen* (Seite 212).

Im Dashboard wird die Anzahl der Computer angezeigt, deren Ereignisanzahl in den vergangenen 7 Tagen einen festgelegten Höchstwert überschritten hat.

Sie können einstellen, dass die von Ihnen ausgewählten Empfänger über Application Control-Ereignisse benachrichtigt werden. Mehr dazu erfahren Sie unter *Einrichten von Application Control-Alerts und -Benachrichtigungen* (Seite 205).

7.4.2 Auswählen von Controlled Applications

Bei rollenbasierter Verwaltung:

- Zur Konfiguration einer Application Control-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellungen – Application Control** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Standardmäßig sind alle Anwendungen zugelassen. Sie können die Anwendungen, die Sie kontrollieren möchten, folgendermaßen wählen:

1. Prüfen Sie, welche Application Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Application Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Application Control-Richtlinie** auf die Registerkarte **Autorisierungen**.
4. Wählen Sie einen **Anwendungstyp**, z.B. **Dateifreigabe**.

   Eine vollständige Liste der Anwendungen in dieser Gruppe wird in der Liste **Zugelassen** angezeigt.

   - Um eine Anwendung zu sperren, wählen Sie sie und verschieben Sie sie in die Liste **Gesperrt**, indem Sie auf die Schaltfläche „Hinzufügen“ klicken.

   - Um neue Anwendungen zu sperren, die Sophos zu diesem Typ in Zukunft hinzufügt, verschieben Sie **Von Sophos zukünftig hinzugefügt** in die Liste **Blockiert**.
   - Um alle Anwendungen dieses Typs zu blockieren, verschieben Sie alle Anwendungen aus der Liste **Zugelassen** in die Liste **Gesperrt**, indem Sie auf die Schaltfläche „Alle hinzufügen“ klicken.

5. Stellen Sie sicher, dass auf der Registerkarte **Scans** im Dialogfeld **Application Control-Richtlinie** das Scannen auf Controlled Applications aktiviert ist. (Mehr dazu erfahren Sie im Abschnitt *Scannen auf Controlled Applications* (Seite 154).) Klicken Sie auf **OK**.

7.4.3 Scannen auf Controlled Applications

Bei rollenbasierter Verwaltung:

- Zur Konfiguration einer Application Control-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellungen – Application Control** verfügen.

- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können Sophos Endpoint Security and Control dazu konfigurieren, Ihr Netzwerk bei Zugriff auf Controlled Applications zu scannen.

1. Prüfen Sie, welche Application Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Application Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Application Control-Richtlinie** wird angezeigt.

3. Legen Sie auf der Registerkarte **Scans** folgende Optionen fest:

   - Zur Aktivierung von On-Access-Scans markieren Sie die Option **On-Access-Scans aktivieren**. Wenn Anwendungen erkannt, jedoch nicht gesperrt werden sollen, markieren Sie die Option **Erkennen, aber laufen lassen**.
   - Zum Aktivieren von On-Demand-Scans und geplanten Scans aktivieren Sie das Kontrollkästchen **On-Demand-Scans und geplante Scans aktivieren**.

   Hinweis: Ihre Einstellungen für die Antivirus- und HIPS-Richtlinie bestimmen, welche Dateien gescannt werden (d.h. die Erweiterungen und Ausnahmen).

Wenn Sie Controlled Applications entfernen möchten, die auf Ihren Netzwerkcomputern gefunden wurden, folgen Sie den Anweisungen im Abschnitt *Deinstallieren unerwünschter Controlled Applications* (Seite 155).

Sie können auch Benachrichtigungen an bestimmte Benutzer senden, wenn auf einem der Computer in der Gruppe eine Controlled Application entdeckt wurde. Anweisungen hierzu finden Sie unter *Einrichten von Application Control-Alerts und -Benachrichtigungen* (Seite 205).

7.4.4 Deinstallieren unerwünschter Controlled Applications

Vor der Deinstallation von Controlled Applications müssen Sie sicherstellen, dass On-Access-Scans für Controlled Applications deaktiviert sind. Bei On-Access-Scans werden Programme gesperrt, die zur Installation und Deinstallation von Anwendungen benötigt werden. Diese Scan-Funktion kann daher die Deinstallation beeinträchtigen.

Es gibt zwei Methoden zum Entfernen von Anwendungen:

- Führen Sie an das Deinstallationsprogramm für das Produkt auf allen Computern aus. Dies erfolgt gewöhnlich über das Programm „Software“ in der Windows-Systemsteuerung.
- Auf dem Server können Sie das Deinstallationsprogramm für das Produkt auf Ihren Computern im Netzwerk über Ihr übliches Skript- oder Administrationstool ausführen.

Sie können die On-Access-Scans für Controlled Applications nun aktivieren.

7.5 Konfigurieren der Data Control-Richtlinie

7.5.1 Data Control

Hinweis: Die Funktion ist nicht im Umfang aller Lizenzen enthalten. Wenn Sie die Funktion nutzen möchten, müssen Sie eine entsprechende Lizenz erwerben. Nähere Informationen finden Sie unter *http://www.sophos.com/de-de/products/complete/comparison.aspx*.

Data Control überwacht und reguliert Dateien mit sensiblen Daten und verhindert so ungewollte Datenverluste über Computer. Sie können Data Control-Regeln erstellen und sie in die **Data Control**-Richtlinien aufnehmen.

Sie können die Übertragung von Dateien auf bestimmte Speichermedien (z.B. Wechselmedien und optische Laufwerke) oder den Transfer von Dateien von bestimmten Anwendungen (z.B. E-Mail-Programmen oder Browser) überwachen und regeln.

Zur Gewährleistung der prompten Definition und Bereitstellung einer Data Control-Richtlinie verfügen die SophosLabs über eine Datenbank mit Definitionen sensibler Daten (Content Control Lists). Die Datenbank umfasst hauptsächlich personenbezogene Daten, beinhaltet jedoch auch andere gängige Datenstrukturen. Wie nachfolgend beschrieben, können Sie Content Control Lists in Enterprise Console integrieren.

7.5.2 Funktionsweise von Data Control

Durch Data Control lassen sich unerwünschte Datenverluste feststellen, die in der Regel durch den falschen Umgang mit sensiblen Daten im Unternehmen verursacht werden. Beispiel: Ein Benutzer versendet eine Datei mit sensiblen Daten über ein Internet-E-Mail-Programm an eine private E-Mail-Adresse.

Data Control ermöglicht die Überwachung und Kontrolle von Dateiübertragungen von Computern auf Speichergeräte und Anwendungen, die mit dem Internet verbunden sind.

- **Speichergeräte:** Data Control fängt alle Dateien ab, die mit Windows Explorer auf ein überwachtes Speichergerät kopiert werden (einschließlich des Windows-Desktops). Dateien, die jedoch direkt in einer Anwendung (z.B. Microsoft Word) gespeichert oder über die Befehlszeile übertragen werden, werden nicht erfasst.

  Über die beiden folgenden Optionen können Sie erzwingen, dass alle Übertragungen auf ein überwachtes Speichergerät mit Windows Explorer erfolgen: **Benutzerbestätigte Übertragungen zulassen und Ereignis protokollieren** oder **Übertragung sperren und Ereignis protokollieren**. Bei Auswahl beider Optionen blockiert Data Control Versuche, Dateien direkt in einer Anwendung zu speichern oder über die Befehlszeile zu übertragen. Der Benutzer wird in einer Desktop-Benachrichtigung aufgefordert, die Übertragung mit Windows Explorer durchzuführen.

  Wenn eine Data Control-Richtlinie nur Regeln mit der Maßnahme **Dateiübertragung zulassen und Ereignis protokollieren** umfasst, greift Data Control nicht beim Speichern in einer Anwendung oder der Übertragung über die Befehlszeile. Benutzer können Speichergeräte somit uneingeschränkt nutzen. Bei Übertragungen mit Windows Explorer werden jedoch weiterhin Data Control-Ereignisse protokolliert.

Hinweis: Diese Einschränkung gilt nicht für die Überwachung von Anwendungen.

- **Anwendungen:** Damit nur von Benutzern eingeleitete Dateiübertragungen überwacht werden, werden einige Systemdateiverzeichnisse von Data Control ausgeschlossen. Auf diese Weise wird die Anzahl der Data Control-Ereignisse auf Dateiübertragungen vonseiten der Benutzer reduziert; von Anwendungen geöffnete Konfigurationsdateien lösen keine Data Control-Ereignisse mehr aus.

  Wichtig: Sollte eine Anwendung beim Öffnen einer Konfigurationsdatei dennoch ein Ereignis auslösen, kann das Problem in der Regel durch das Ausschließen bestimmter Verzeichnisse oder durch Desensibilisierung der Data Control-Regel behoben werden. Weitere Informationen finden Sie im Support-Artikel 113024 (*http://www.sophos.de/support/knowledgebase/article/113024.html*).

  Hinweis: Wenn Sie Remote-Dateien in der Antivirus- und HIPS-Richtlinie von On-Access-Scans ausschließen, werden Dateien, die mit einer überwachten Anwendung, z.B. einem E-Mail-Client, Browser oder Instant Messaging-Client hochgeladen oder angehängt wurden, nicht von Sophos Data Control erfasst. Data Control verwendet die gleichen Ausschlüsse wie der On-Access-Scanner von Sophos Anti-Virus: Wenn das Scannen von Remote-Dateien also deaktiviert wurde, werden keine Remote-Dateien an Data Control gesendet. Diese Einschränkung gilt nicht für die Überwachung von Speichergeräten. Weitere Informationen zum Konfigurieren von On-Access-Scans entnehmen Sie bitte dem Abschnitt *Ausschließen von Objekten von On-Access-Scans* (Seite 103).

Data Control-Richtlinien

Data Control dient der Überwachung und Kontrolle des Datenverkehrs durch Festlegen von Data Control-Richtlinien und deren Übertragung auf Netzwerkgruppen und -computer.

Wichtig: Data Control läuft nicht unter Windows 2008 Server Core. Daher muss diese Funktion auf Computern mit diesem Betriebssystem deaktiviert werden. Um Computer mit Windows 2008 Server Core von Data Control auszuschließen, gliedern Sie diese in eine Gruppe ein, in deren Data Control-Richtlinie diese Funktion deaktiviert ist. Mehr dazu erfahren Sie unter *Aktivieren/Deaktivieren von Data Control* (Seite 161).

Data Control-Richtlinien umfassen eine oder mehrere Regeln, in denen die Zustände definiert werden. Außerdem sind die zu ergreifenden Maßnahmen für den Fall festgelegt, dass eine Übereinstimmung mit der Regel vorliegt. Eine Data Control-Regel kann mehreren Richtlinien angehören.

Wenn eine Data Control-Richtlinie mehrere Regeln umfasst, liegt bereits ein Richtlinienverstoß vor, wenn eine Datei die Kriterien *einer* Regel der Data Control-Richtlinie erfüllt.

Data Control-Regelbedingungen

Die Data Control-Richtlinien umfassen Ziel, Dateiname, Erweiterung, Dateityp und Inhalt der Datei.

Ziele umfassen Geräte (z.B. Wechselmedien wie etwa USB-Flashlaufwerke) und Anwendungen (z.B. Internet-Browser oder E-Mail-Clients).

Der Abgleich von Dateiinhalten wird über Content Control Lists definiert. Hierbei handelt es sich um die Beschreibung strukturierter Daten auf XML-Basis. SophosLabs stellen eine Vielzahl an Content Control Lists bereit, die sich in Data Control-Regeln integrieren lassen.

Weitere Informationen zu Data Control-Regeln und Bedingungen, die für Dateien gelten, finden Sie unter *Data Control-Regeln* (Seite 159).

Mehr zu Content Control Lists (CCLs) zur Definition von Dateiinhalten erfahren Sie unter *Content Control Lists* (Seite 159).

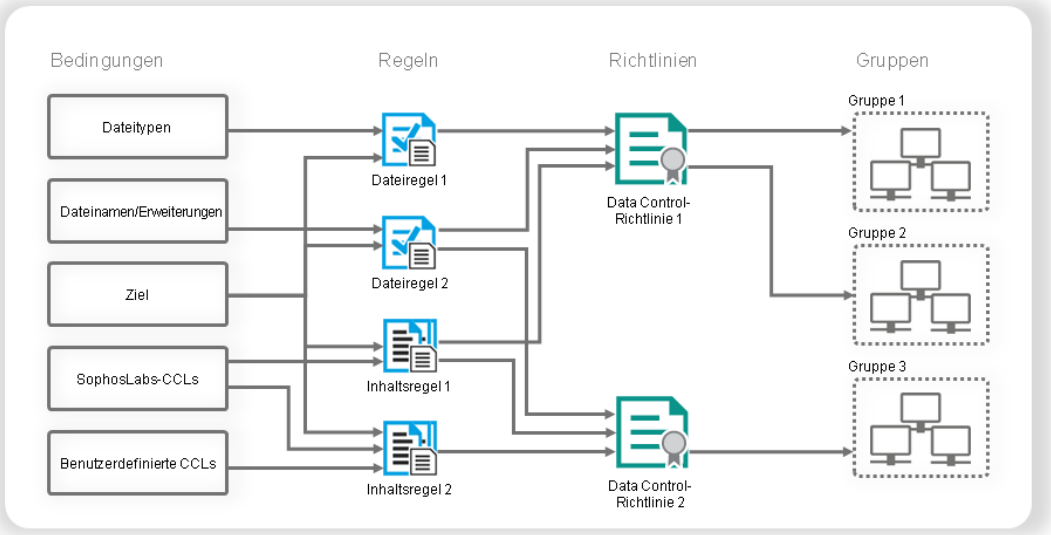


Abbildung 2: Data Control

Data Control-Regelmaßnahmen

Wenn Data Control alle in einer Regel festgelegten Bedingungen vorfindet, liegt eine Übereinstimmung mit der Regel vor. Data Control ergreift dann die in der Regel bestimmten Maßnahmen und verzeichnet das Ereignis im Protokoll. Sie können eine der folgenden Maßnahmen festlegen:

- Dateiübertragung zulassen und Ereignis protokollieren
- Benutzerbestätigte Übertragungen zulassen und Ereignis protokollieren
- Übertragung sperren und Ereignis protokollieren

Wenn eine Datei zwei Data Control-Regeln entspricht, greift die Regel mit der strengeren Maßnahme. Data Control-Regeln, die die Dateiübertragung blockieren, haben Vorrang vor Regeln, die die Dateiübertragung bei entsprechender Bestätigung durch den Benutzer erlauben. Regeln, die die Dateiübertragung bei entsprechender Bestätigung durch den Benutzer erlauben, haben wiederum Vorrang vor Regeln, die die Dateiübertragung zulassen.

Wenn eine Übereinstimmung mit einer Regel vorliegt und die Übertragung einer Datei gesperrt wird bzw. vom Benutzer bestätigt werden muss, wird standardmäßig eine Desktop-Benachrichtigung auf dem Endpoint angezeigt. Die Benachrichtigung weist auch auf die entsprechende Regel hin. Sie können Ihre eigenen Benachrichtigungen für blockierte Dateiübertragungen und für den Fall erstellen, dass der Benutzer die Dateiübertragung bestätigen soll. Nähere Informationen finden Sie unter *Einrichten von Data Control-Alerts und -Benachrichtigungen* (Seite 206).

7.5.3 Data Control-Regeln

In Data Control-Regeln werden die Bedingungen festgelegt, die Data Control-Scans erkennen sollen. Ferner werden bei Regelübereinstimmung zu ergreifende Maßnahmen definiert und von Scans auszuschließende Dateien festgelegt.

Sie können eigene Regeln erstellen oder die vordefinierten Regeln von Sophos übernehmen. Sophos bietet vordefinierte Data Control-Regeln, die Sie nach Belieben an Ihre Bedürfnisse anpassen können. Die Regeln dienen lediglich der Veranschaulichung und werden nicht von Sophos aktualisiert.

Es wird zwischen *Dateiregeln* und *Inhaltsregeln* unterschieden.

Dateiregeln

In *Dateiregeln* wird die Maßnahme (z.B. Datenübertragung an Wechselmedien blockieren) festgelegt, die ergriffen wird, wenn ein Benutzer versucht, eine Datei eines bestimmten Namens oder Typs (True File Type, z.B. eine Tabelle) an ein angegebenes Ziel zu übertragen.

Data Control umfasst True-File-Type-Definitionen für über 150 verschiedene Dateiformate. Unter Umständen werden bisweilen weitere True-File-Type-Definitionen hinzugefügt. Neue Dateitypen werden automatisch in die Data Control-Regeln der entsprechenden True-File-Type-Kategorie aufgenommen.

Dateitypen, die nicht von der True-File-Type-Definition erfasst werden, lassen sich anhand ihrer Erweiterung bestimmen.

Inhaltsregeln

Inhaltsregeln umfassen mindestens eine Content Control List. Hierin wird die Maßnahme festgelegt, die ergriffen wird, wenn ein Benutzer versucht, Daten, die mit allen Content Control Lists übereinstimmen, an den angegebenen Zielort zu übertragen.

7.5.4 Content Control Lists

Content Control Lists (CCL) umfassen Bedingungen zur Beschreibung strukturierter Dateiinhalte. Content Control Lists können sich auf einen Datentyp beschränken (z.B. eine Anschrift oder Sozialversicherungsnummer) oder eine Kombination verschiedener Daten umfassen (z.B. Projektnamen, die „vertraulich“ oder ähnlich lauten).

Sie können auf die von Sophos bereitgestellten *SophosLabs Content Control Lists* zurückgreifen oder eigene Content Control Lists erstellen.

SophosLabs Content Control Lists umfassen Definitionen zu gängigen finanziellen und personenbezogenen Datentypen (z.B. Kreditkartennummern, Sozialversicherungsnummern, Anschriften oder E-Mail-Adressen). Die Präzision der Erkennung sensibler Daten in SophosLabs Content Control Lists wird durch den Einsatz diverser Technologien, wie etwa Prüfsummen, optimiert.

SophosLabs Content Control Lists können nicht bearbeitet werden. Auf Wunsch können Sie jedoch die Erstellung einer neuen SophosLabs Content Control List bei Sophos beantragen. Nähere Informationen finden Sie im Support-Artikel 51976 (*http://www.sophos.de/support/knowledgebase/article/51976.html*).

Hinweis: Double-Byte-Zeichen (z.B. japanische oder chinesische Zeichen) werden in der aktuellen Version der Content Control Lists nicht offiziell unterstützt. Im Content Control List Editor können Sie jedoch Double-Byte-Zeichen eingeben.

Mengenfestlegung für SophosLabs Content Control Lists

Den meisten SophosLabs Content Control Lists wurden *Mengenwerte* zugewiesen.

Mengen definieren sich als der Umfang an Content Control List-Schlüsseldaten, die eine Datei umfassen muss, damit eine Übereinstimmung mit der Content Control List vorliegt. Sie können den Mengenwert einer SophosLabs Content Control List in einer Dateiregel ändern, die die Content Control List umfasst.

Mit Mengenwerten können Sie Data Control an Ihre Bedürfnisse anpassen und so vermeiden, dass Dokumente gesperrt werden, die keine sensiblen Daten enthalten (z.B. ein Dokument, das eine Anschrift und eine oder zwei Telefonnummern in der Kopf- oder Fußzeile umfasst). Wenn Sie nur nach einer Anschrift suchen, liegt möglicherweise bei zahlreichen Dokumenten eine Regelübereinstimmung vor, und es werden entsprechend viele Data Control-Ereignisse angezeigt. Um jedoch den Verlust wichtiger Kundendaten zu vermeiden, empfiehlt sich etwa, lediglich die Übertragung von Dokumenten mit 50 Anschriften und mehr zu sperren. In anderen Fällen kann es sich wiederum anbieten, nur nach einem Datenvorkommen zu suchen (z.B. einer Kreditkartennummer).

7.5.5 Data Control-Ereignisse

Data Control-Ereignisse (z.B. Kopieren einer Datei mit sensiblen Daten auf ein USB-Flash-Laufwerk) werden an Enterprise Console übermittelt und können in der **Ereignisanzeige von Data Control** angezeigt werden. Die Ereignisse werden auch auf dem Endpoint protokolliert. Benutzer, die über die erforderlichen Rechte verfügen, können die Ereignisse in Endpoint Security and Control aufrufen.

Hinweis: Endpoints können bis zu 50 Data Control-Ereignisse pro Stunde an Enterprise Console senden. Alle Ereignisse werden lokal auf dem Endpoint protokolliert.

Im Dialogfeld **Data Control – Ereignisanzeige** können Sie Filter anlegen und sich nur Ereignisse anzeigen lassen, die für Sie relevant sind. Außerdem können Sie die Liste der Data Control-Ereignisse in eine Datei exportieren oder in die Zwischenablage kopieren. Nähere Informationen hierzu finden Sie unter *Anzeige von Data Control-Ereignissen* (Seite 213) und *Exportieren der Ereignisliste in eine Datei* (Seite 222).

Auf dem Dashboard wird die Anzahl der Computer angezeigt, auf denen die Summe der Data Control-Ereignisse in den vergangenen 7 Tagen den angegebenen Höchstwert überschritten hat. Nähere Informationen zum Festlegen des Höchstwerts finden Sie im Abschnitt *Konfigurieren des Dashboards* (Seite 56).

Zudem können Sie festlegen, dass die gewählten Empfänger über Data Control-Ereignisse benachrichtigt werden. Mehr dazu erfahren Sie unter *Einrichten von Data Control-Alerts und -Benachrichtigungen* (Seite 206).

7.5.6 Aktivieren/Deaktivieren von Data Control

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Device Control-Richtlinie ist die Berechtigung **Richtlinieneinstellung – Data Control** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Data Control ist standardmäßig deaktiviert und die Dateiübertragung im Netzwerk wird nicht durch Regeln überwacht bzw. eingeschränkt.

So aktivieren Sie Data Control:

1. Prüfen Sie, welche Data Control-Richtlinie von der/den Computergruppe/n verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Data Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Data Control-Richtlinie** wird angezeigt.
3. Aktivieren Sie auf der Registerkarte **Richtlinienregeln** das Kontrollkästchen **Data Control aktivieren**.
4. Klicken Sie auf die Schaltfläche **Regel hinzufügen**. Wählen Sie im Dialogfeld **Verwaltung der Data Control-Regeln** die Regeln aus, die Sie zu der Richtlinie hinzufügen möchten und klicken Sie auf **OK**.

   Wichtig: Solange Sie keine Data Control-Regeln hinzufügen, werden Dateien nicht von Data Control überwacht.

Wenn Sie Data Control zu einem späteren Zeitpunkt deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Data Control aktivieren**.

7.5.7 Erstellen einer Dateiregel

Bei rollenbasierter Verwaltung:

- Zum Erstellen bzw. Ändern von Dateiregeln für Data Control müssen Sie über die Berechtigung **Data Control – Anpassung** verfügen.
- Zum Einrichten von Data Control-Richtlinien müssen Sie über die Berechtigung **Richtlinieneinstellungen – Data Control** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Eine Übersicht über Dateiregeln finden Sie unter *Data Control-Regeln* (Seite 159).

So können Sie eine Dateiregel erstellen und zu einer Data Control-Richtlinie hinzufügen:

1. Prüfen Sie, welche Data Control-Richtlinie von der/den Computergruppe/n verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

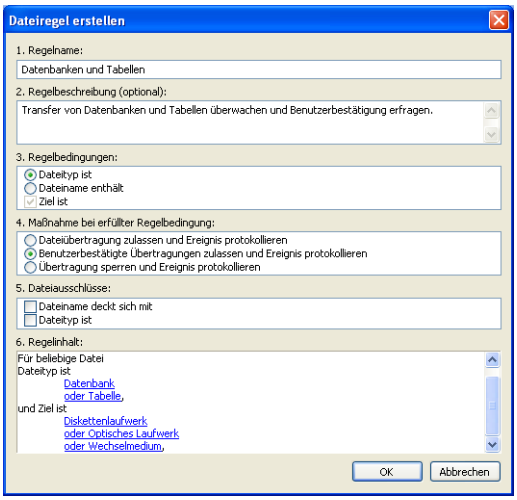
   Sie können jedoch auch eine Regel im Menü **Extras** erstellen und sie zu einem späteren Zeitpunkt zu einer oder mehreren Richtlinien hinzufügen. Richten Sie den Mauszeiger im **Extras**-Menü auf **Data Control**. Klicken Sie anschließend auf die Option **Data Control-Regeln** und führen Sie die Schritte 4 bis 10 durch.
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Data Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Öffnen Sie im Dialogfeld **Data Control-Richtlinie** die Registerkarte **Richtlinienregeln**. Wählen Sie die Option **Data Control aktivieren** und klicken Sie anschließend auf **Regeln verwalten**.
4. Klicken Sie im Dialogfeld **Verwaltung der Data Control-Regeln** auf die Option **Dateiregel hinzufügen**.
5. Geben Sie im Dialogfeld **Dateiregel erstellen** unter **Regelname** einen Regelnamen ein.
6. Im Bereich **Beschreibung der Regel (optional)** können Sie die Regel auf Wunsch beschreiben.
7. Legen Sie im Bereich **Regelbedingungen:** die gewünschten Regelbedingungen fest.

   Die Zielbedingung ist vordefiniert und muss Bestandteil der Regel sein.

   Standardmäßig werden alle Dateitypen gescannt. Wenn nur bestimmte Dateitypen gescannt werden sollen, klicken Sie auf **Dateityp ist**. Nun können Sie die Bedingung an Ihre Wünsche anpassen (siehe Schritt 10).
8. Wählen Sie im Bereich **Maßnahme bei erfüllter Regelbedingung:** die gewünschte Maßnahme aus.
9. Wenn Dateien nicht von Data Control erfasst werden sollen, aktivieren Sie im Bereich **Dateiausschlüsse:** das Kontrollkästchen **Datei deckt sich mit** oder **Dateityp ist**.

10. Klicken Sie im Bereich **Regelinhalt** alle unterstrichenen Werte an und legen Sie die Regelbedingungen fest.
    Wenn Sie beispielsweise auf **Ziel auswählen** klicken, öffnet sich das Dialogfeld **Zieltypbedingung**. In diesem Feld können Sie Geräte und/oder Anwendungen auswählen, zu denen der Datenverkehr eingeschränkt werden soll.

    Wählen Sie Bedingungen für alle unterstrichenen Werte aus bzw. geben Sie diese ein.



    Klicken Sie auf **OK**.

    Die neue Regel wird im Dialogfeld **Verwaltung der Data Control-Regeln** angezeigt.

11. Aktivieren Sie zum Hinzufügen der Regel zur Richtlinie das Kontrollkästchen neben dem Regelnamen und klicken Sie auf **OK**.

    Die Regel wird zur Data Control-Richtlinie hinzugefügt.

Sie können Alerts und Benachrichtigungen an den Benutzer senden, wenn eine Übereinstimmung mit einer Regel in der Data Control-Richtlinie vorliegt. Mehr dazu erfahren Sie unter *Einrichten von Data Control-Alerts und -Benachrichtigungen* (Seite 206).

7.5.8 Erstellen einer Inhaltsregel

Bei rollenbasierter Verwaltung:

- Zum Erstellen bzw. Ändern von Dateiregeln und Content Control Lists für Data Control müssen Sie über die Berechtigung **Data Control – Anpassung** verfügen.
- Zum Einrichten von Data Control-Richtlinien müssen Sie über die Berechtigung **Richtlinieneinstellungen – Data Control** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Eine Übersicht über Inhaltsregeln und Content Control Lists finden Sie unter *Data Control-Regeln* (Seite 159).

So können Sie eine Inhaltsregel erstellen und zu einer Data Control-Richtlinie hinzufügen:

1. Prüfen Sie, welche Data Control-Richtlinie von der/den Computergruppe/n verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

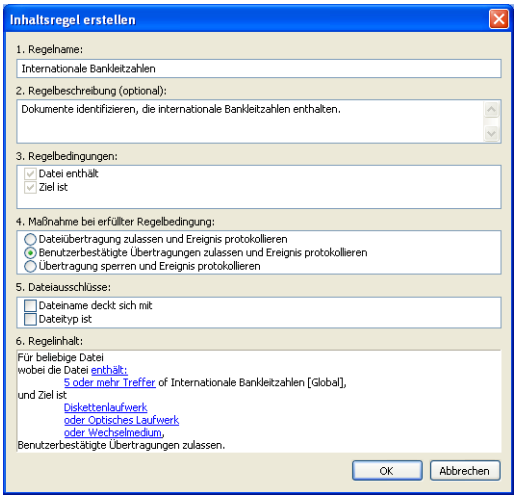
   Sie können jedoch auch eine Regel im Menü **Extras** erstellen und sie zu einem späteren Zeitpunkt zu einer oder mehreren Richtlinien hinzufügen. Richten Sie den Mauszeiger im **Extras**-Menü auf **Data Control**. Klicken Sie anschließend auf die Option **Data Control-Regeln** und führen Sie die Schritte 4 bis 13 durch.
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Data Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Öffnen Sie im Dialogfeld **Data Control-Richtlinie** die Registerkarte **Richtlinienregeln**. Wählen Sie die Option **Data Control aktivieren** und klicken Sie anschließend auf **Regeln verwalten**.
4. Klicken Sie im Dialogfeld **Verwaltung der Data Control-Regeln** auf die Option **Inhaltsregel hinzufügen**.
5. Geben Sie im Dialogfeld **Dateiregel erstellen** unter **Regelname** einen Regelnamen ein.
6. Im Bereich **Beschreibung der Regel (optional)** können Sie die Regel auf Wunsch beschreiben.
7. Im Bereich **Regelbedingungen** sind die Dateiinhalt- und Zielbedingungen bereits ausgewählt. Für eine Inhaltsregel müssen Sie beide Bedingungen festlegen.
8. Wählen Sie im Bereich **Maßnahme bei erfüllter Regelbedingung:** die gewünschte Maßnahme aus.
9. Wenn Dateien nicht von Data Control erfasst werden sollen, aktivieren Sie im Bereich **Dateiausschlüsse:** das Kontrollkästchen **Datei deckt sich mit** oder **Dateityp ist**.
10. Klicken Sie im Bereich **Regelinhalt** auf den unterstrichenen Wert „Dateiinhalt auswählen“.
11. Wählen Sie im Dialogfeld **Content Control List – Verwaltung** die Content Control Lists aus, die Sie in die Regel aufnehmen möchten.

    Wenn Sie eine SophosLabs Content Control-Liste erstellen möchten, wählen Sie die Liste für Ihr Land oder eine globale Content Control List aus.

    Anweisungen zum Erstellen einer neuen Content Control List finden Sie unter *Erstellen/Ändern einer einfachen Content Control List* (Seite 167) und *Erstellen/Ändern einer komplexen Content Control List* (Seite 169).

    Klicken Sie auf **OK**.
12. Wenn Sie die Menge ändern möchten, die einer SophosLabs Content Control List zugewiesen ist, klicken Sie unter **Regelinhalt** auf den unterstrichenen „Menge“-Wert („mindestens *n* Treffer“), den Sie ändern möchten. Geben Sie im Dialogfeld **Mengen-Editor** einen neuen Mengenwert ein.

13. Wählen Sie im Bereich **Regelinhalt** Bedingungen für die verbleibenden unterstrichenen Werte aus bzw. geben Sie sie ein.



Klicken Sie auf **OK**.

Die neue Regel wird im Dialogfeld **Verwaltung der Data Control-Regeln** angezeigt.

14. Aktivieren Sie zum Hinzufügen der Regel zur Richtlinie das Kontrollkästchen neben dem Regelnamen und klicken Sie auf **OK**.

Die Regel wird zur Data Control-Richtlinie hinzugefügt.

Sie können Alerts und Benachrichtigungen an den Benutzer senden, wenn eine Übereinstimmung mit einer Regel in der Data Control-Richtlinie vorliegt. Mehr dazu erfahren Sie unter *Einrichten von Data Control-Alerts und -Benachrichtigungen* (Seite 206).

7.5.9 Hinzufügen einer Data Control-Regel zu einer Richtlinie

Bei rollenbasierter Verwaltung:

- Hierzu müssen Sie über die Berechtigung **Richtlinieneinstellung – Data Control** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So fügen Sie einer Richtlinie eine Data Control-Regel hinzu:

1. Prüfen Sie, welche Data Control-Richtlinie von der/den Computergruppe/n verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Data Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Data Control-Richtlinie** wird angezeigt.

3. Klicken Sie im Fenster **Richtlinienregeln** auf **Hinzufügen**.

   Das Dialogfeld **Verwaltung der Data Control-Regeln** wird angezeigt.

4. Wählen Sie die gewünschten Regeln aus und klicken Sie auf **OK**.

7.5.10 Entfernen einer Data Control-Regel aus einer Richtlinie

Bei rollenbasierter Verwaltung:

- Hierzu müssen Sie über die Berechtigung **Richtlinieneinstellung – Data Control** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So entfernen Sie eine Data Control-Regel aus einer Richtlinie:

1. Prüfen Sie, welche Data Control-Richtlinie von der/den Computergruppe/n verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Data Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Data Control-Richtlinie** wird angezeigt.

3. Wählen Sie auf der Registerkarte **Richtlinienregeln** die Regel aus, die Sie löschen möchten, und klicken Sie auf **Entfernen**.

7.5.11 Ausschließen von Dateien oder Dateitypen aus Data Control

Bei rollenbasierter Verwaltung gilt als Voraussetzung für das Ausschließen von Dateien aus Data Control die Berechtigung **Data Control – Anpassung**. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wenn Sie Dateien und Dateitypen von Data Control ausschließen möchten, müssen Sie in einer Data Control-Regel Ausnahmen definieren.

Schließen Sie Dateien bzw. Dateitypen in Regeln mit höchster Priorität (d.h. mit den strengsten Maßnahmen) aus.

So schließen Sie Dateien oder Dateitypen aus Data Control aus:

1. Wählen Sie im Menü **Extras** unter **Data Control** die Option **Data Control-Regeln**.
2. Wählen Sie im Dialogfeld **Verwaltung der Data Control-Regeln** die zu ändernde Regel aus und klicken Sie auf **Ändern**. Sie können jedoch auch per Klick auf **Dateiregel hinzufügen** oder **Inhaltsregel hinzufügen** eine neue Regel erstellen.
3. Aktivieren Sie im **Regel-Editor** unter **Dateiausschlüsse** das Kontrollkästchen **Datei deckt sich mit**.
4. Klicken Sie im Bereich **Regelinhalt** auf den unterstrichenen Wert, um die Namen der auszuschließenden Dateien anzugeben.

5. Klicken Sie im Dialogfeld **Dateinamensbedingung ausschließen** auf **Hinzufügen** und geben Sie die Namen der Dateien an, die Sie ausschließen möchten.

   Sie können die Platzhalter * und ? benutzen.

   Der Platzhalter ? kann nur für Dateinamen oder Erweiterungen benutzt werden. Er ersetzt in der Regel ein einziges Zeichen. Am Ende eines Dateinamens kann das Fragezeichen jedoch auch ein fehlendes Zeichen ersetzen. Beispiel: Die Eingabe von „datei??.txt“ dient als Ersatz für „datei.txt“, „datei1.txt“ sowie „datei12.txt“, jedoch nicht „datei123.txt“.

   Der Platzhalter * kann nur für Dateinamen oder -erweiterungen in der Form [Dateiname].* oder *.[Erweiterung] verwendet werden. Beispiel: Die Eingabe von „datei*.txt“, „datei.txt*“ und „datei.*txt“ ist nicht zulässig.
6. Aktivieren Sie im **Regel-Editor** unter **Dateiausschlüsse** das Kontrollkästchen **Dateityp ist**.
7. Klicken Sie im Bereich **Regelinhalt** auf den unterstrichenen Wert, um die auszuschließenden Dateitypen anzugeben.
8. Wählen Sie im Dialogfeld **Dateinamensbedingung ausschließen** die auszuschließenden Dateitypen und klicken Sie auf **OK**.

7.5.12 Importieren/Exportieren einer Data Control-Regel

Bei rollenbasierter Verwaltung gilt als Voraussetzung für das Importieren/Exportieren einer Data Control-Regel die Berechtigung **Data Control – Anpassung**. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Data Control-Regeln können als XML-Dateien importiert bzw. exportiert werden.

So importieren/exportieren Sie eine Data Control-Regel:

1. Richten Sie den Mauszeiger im Menü **Extras** auf **Data Control**. Klicken Sie anschließend auf die Option **Data Control-Regeln**.
2. Klicken Sie im Dialogfeld **Verwaltung der Data Control-Regeln** auf die Option **Importieren** oder **Exportieren**.
   - Suchen Sie zum Importieren einer Regel die gewünschte Regel im Dialogfeld **Importieren**, wählen Sie die Regel aus und klicken Sie auf **Öffnen**.
   - Wählen Sie zum Exportieren einer Regel im Dialogfeld **Exportieren** einen Speicherort für die Datei aus, geben Sie der Datei einen Namen und klicken Sie auf **Speichern**.

7.5.13 Erstellen/Ändern einer einfachen Content Control List

Bei rollenbasierter Verwaltung gilt als Voraussetzung für die Erstellung einer Content Control List die Berechtigung **Data Control – Anpassung**. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Eine Übersicht über Content Control Lists finden Sie unter *Content Control Lists* (Seite 159).

So erstellen/ändern Sie eine Content Control List:

1. Wählen Sie im Menü **Extras** unter **Data Control** die Option **Data Control Content Control Lists**.

2. Klicken Sie im Dialogfeld **Content Control List - Verwaltung** auf **Hinzufügen**, um eine neue Content Control List zu erstellen, oder wählen Sie eine vorhandene Content Control List aus und klicken Sie auf **Ändern**.
3. Geben Sie im Dialogfeld **Neue Content Control List** in das Feld **Name** eine Bezeichnung für die Content Control List ein.
4. Im Feld **Beschreibung** können Sie die Content Control List auf Wunsch beschreiben.
5. Sie können einer Content Control List Kriterien zuweisen oder vorhandene Kriterien bearbeiten. Klicken Sie hierzu neben dem Feld **Kriterien** auf **Ändern**.

   Anhand von Kriterien können Content Control Lists nach Typ und Geltungsbereich filtern.
6. Wählen Sie im Dialogfeld **Content Control List-Kriterien ändern** die gewünschten Kriterien aus der Liste **Verfügbare Kriterien** aus und verschieben Sie sie in die Liste **Gewählte Kriterien**. Klicken Sie auf **OK**.
7. Wählen Sie im Bereich **Nach Inhaltsübereinstimmung scannen** eine Suchbedingung aus („Beliebiger Ausdruck“, „Alle Ausdrücke“ oder „Dieser Ausdruck“) und geben Sie die gewünschten Suchbegriffe durch Leerzeichen voneinander getrennt ein. Klicken Sie auf **OK**.

   Hinweis: Bei der Suche wird zwischen Groß- und Kleinschreibung unterschrieben.

   Anführungszeichen sind in einfachen Content Control Lists nicht zulässig. Wenn Sie nach einem genauen Wortlaut suchen, wählen Sie die Bedingung „Dieser Ausdruck“.

   Zum Auffinden komplexer Ausdrücke empfiehlt sich die Suche über den Advanced Content Control List Editor, der im Abschnitt *Erstellen/Ändern einer komplexen Content Control List* (Seite 169) beschrieben wird.

Die neue Content Control List wird im Dialogfeld **Content Control List – Verwaltung** angezeigt.

Beispiele

Suchbedingung	Beispiel	Beschreibung
Nach einem der Begriffe	vertraulich geheim	Suche nach Dokumenten, die die Begriffe „vertraulich“ oder „geheim“ beinhalten.
Nach allen Begriffen	Projekt vertraulich	Suche nach Dokumenten, die die Begriffe „Projekt“ und „vertraulich“ beinhalten.
Genaue Entsprechung	nur für den internen Gebrauch	Suche nach Dokumenten, die den Ausdruck „nur für den internen Gebrauch“ beinhalten.

Jetzt können Sie die neue Content Control List einer Inhaltsregel zuweisen.

7.5.14 Erstellen/Ändern einer komplexen Content Control List

Bei rollenbasierter Verwaltung gilt als Voraussetzung für die Erstellung einer Content Control List die Berechtigung **Data Control – Anpassung**. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Eine Übersicht über Content Control Lists finden Sie unter *Content Control Lists* (Seite 159).

Sie können eine Content Control List erstellen, die einen oder mehrere reguläre Ausdrücke und einen Schwellenwert enthält. Verwenden Sie hierzu den Advanced Content Control List Editor.

So erstellen/bearbeiten Sie eine Content Control List mit dem Advanced Content Control List Editor:

1. Wählen Sie im Menü **Extras** unter **Data Control** die Option **Data Control Content Control Lists**.
2. Klicken Sie im Dialogfeld **Content Control List - Verwaltung** auf **Hinzufügen**, um eine neue Content Control List zu erstellen, oder wählen Sie eine vorhandene Content Control List aus und klicken Sie auf **Ändern**.
3. Geben Sie im Dialogfeld **Neue Content Control List** in das Feld **Name** eine Bezeichnung für die Content Control List ein.
4. Im Feld **Beschreibung** können Sie die Content Control List auf Wunsch beschreiben.
5. Sie können einer Content Control List Kriterien zuweisen oder vorhandene Kriterien bearbeiten. Klicken Sie hierzu neben dem Feld **Kriterien** auf **Ändern**.

   Anhand von Kriterien können Content Control Lists nach Typ und Geltungsbereich filtern.
6. Wählen Sie im Dialogfeld **Content Control List-Kriterien ändern** die gewünschten Kriterien aus der Liste **Verfügbare Kriterien** aus und verschieben Sie sie in die Liste **Gewählte Kriterien**. Klicken Sie auf **OK**.
7. Klicken Sie auf **Erweitert**.
8. Klicken Sie im Bereich **Erweitert** auf **Erstellen**, um einen neuen Ausdruck zu erstellen, oder wählen Sie einen vorhandenen Ausdruck aus und klicken Sie auf **Ändern**.
9. Geben Sie in das Dialogfeld **Content Control List – Erweiterte Funktionen** einen regulären Ausdruck mit Perl 5-Syntax ein.

   Nähere Informationen hierzu finden Sie im Begleitmaterial zu Perl oder unter *http://www.boost.org/doc/libs/1_34_1/libs/regex/doc/syntax_perl.html*.
10. Geben Sie in das Feld **Wert** die Zahl ein, die zum Gesamtwert einer Content Control List addiert wird, wenn eine Übereinstimmung mit einem regulären Ausdruck vorliegt.
11. Geben Sie in das Feld **Höchstzahl** die maximal zugelassenen Übereinstimmungen eines regulären Ausdrucks ein, die in die Gesamtbewertung eingehen.
    Bei einem Ausdruck mit der Bewertung 5 und der maximalen Anzahl 2 wird höchstens 10 zur Gesamtbewertung der Content Control List hinzugefügt. Wird der Ausdruck dreimal gefunden, wird dennoch 10 zur Gesamtbewertung addiert.

    Klicken Sie auf **OK**.
12. Wiederholen Sie die Schritte 5 bis 11, wenn Sie weitere reguläre Ausdrücke in die Content Control List aufnehmen möchten.

13. Geben Sie im Feld **Schwellenwert** die erforderliche Trefferanzahl eines regulären Ausdrucks an, damit eine Übereinstimmung mit der Content Control List vorliegt.

    Als Beispiel soll eine Content Control List mit der Schwellenbewertung 8 und drei Ausdrücken (A, B und C) sowie der folgenden Bewertung und maximalen Anzahl betrachtet werden:

Ausdruck	Bewertung	Höchstzahl
Ausdruck A	5	2
Ausdruck B	3	1
Ausdruck C	1	5

    Übereinstimmung mit der Content Control List liegt vor, wenn Data Control zwei Übereinstimmungen mit Ausdruck A oder eine Übereinstimmung mit Ausdruck A und eine Übereinstimmung mit Ausdruck B oder eine Übereinstimmung mit Ausdruck B und fünf Übereinstimmungen mit Ausdruck C findet.

    Klicken Sie auf **OK**.

Die neue Content Control List wird im Dialogfeld **Content Control List-Verwaltung** angezeigt.

Beispiel eines regulären Ausdrucks

(?i)\b[a-ceghj-npr-tw-z][a-ceghj-npr-tw-z]\s?\d{2}\s?\d{2}\s?\d{2}\s?[abcd]?\b

Dieser reguläre Ausdruck stimmt mit Sozialversicherungsnummern aus Großbritannien überein, z.B. AA 11 11 11 A.

(?i)	Groß- und Kleinschreibung wird ignoriert.
\b	Sucht nach dem Übergang von einem Wortzeichen zu einem Nicht-Wort-Zeichen.
[a-ceghj-npr-tw-z]	Sucht innerhalb des Buchstabenbereichs (A bis C E G H J bis N P R bis T W bis Z) nach einem einzelnen Zeichen.
?	Keine oder eine Übereinstimmung mit dem vorherigen Element.
\s?	Entspricht Null oder Leerschritt.
\d{2}	Entspricht zwei Ziffern.
[abcd]	Sucht in der Liste nach einem einzelnen Zeichen (A, B, C oder D).

Jetzt können Sie die neue Content Control List einer Inhaltsregel zuweisen.

7.5.15 Importieren/Exportieren einer Content Control List

Bei rollenbasierter Verwaltung gilt als Voraussetzung für das Importieren/Exportieren einer Content Control List die Berechtigung **Data Control – Anpassung**. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Content Control Lists können als XML-Dateien importiert bzw. exportiert werden. Sie können Content Control Lists zwischen Sophos Produkten austauschen, die sie unterstützen.

Hinweis: SophosLabs Content Control Lists können nicht exportiert werden.

So importieren/exportieren Sie eine Content Control List:

1. Wählen Sie im Menü **Extras** unter **Data Control** die Option **Data Control Content Control Lists**.
2. Klicken Sie im Dialogfeld **Content Control List – Verwaltung** auf die Option **Importieren** oder **Exportieren**.
   - Wählen Sie zum Importieren einer Content Control List im Dialogfeld **Importieren** die gewünschte Liste aus und klicken Sie auf **Öffnen**.
   - Wählen Sie zum Exportieren einer Content Control List im Dialogfeld **Exportieren** einen Speicherort für die Datei aus, geben Sie der Datei einen Namen und klicken Sie auf **Speichern**.

7.6 Konfigurieren der Device Control-Richtlinie

7.6.1 Device Control

Hinweis: Die Funktion ist nicht im Umfang aller Lizenzen enthalten. Wenn Sie die Funktion nutzen möchten, müssen Sie eine entsprechende Lizenz erwerben. Nähere Informationen finden Sie unter *http://www.sophos.com/de-de/products/complete/comparison.aspx*.

Wichtig: Es ist davon abzuraten, Sophos Device Control mit Gerätesteuerungssoftware anderer Anbieter zu kombinieren.

Mit Device Control können Sie verhindern, dass Benutzer nicht zugelassene externe Hardware, Wechselmedien und Wireless-Geräte auf dem Computer einsetzen. So wird das Risiko unerwünschter Datenverluste minimiert. Zudem wird die unzulässige Installation unternehmensfremder Software unterbunden.

Wechselmedien, optische Disk-Laufwerke und Diskettenlaufwerke können auch schreibgeschützt werden.

Mit Device Control können Sie das Risiko von Netzwerkbrücken zwischen einem Unternehmensnetzwerk und einem unternehmensfremden Netzwerk minimieren. Der Modus **Netzwerkbrücken sperren** steht für Wireless-Geräte und Modems zur Verfügung. Hierbei werden Wireless- oder Modemnetzwerkadapter deaktiviert, wenn ein Endpoint an ein physisches Netzwerk angeschlossen wird (in der Regel per Ethernet-Verbindung). Wenn der Endpoint von dem physischen Netzwerk getrennt wird, wird der Wireless- oder Modemnetzwerkadapter wieder aktiviert.

Device Control ist standardmäßig deaktiviert und alle Geräte sind zugelassen.

Für den ersten Einsatz von Device Control empfiehlt sich:

- Wählen Sie Gerätearten aus, die überwacht werden sollen.
- Lassen Sie Geräte zwar erkennen, jedoch nicht blockieren.
- Die Device Control-Ereignisse können Ihnen die Entscheidung erleichtern, welche Gerätearten gesperrt oder von Device Control nicht berücksichtigt werden sollen.
- Lassen Sie Device Control Speichermedien erkennen und blockieren oder schreibschützen Sie sie.

Nähere Informationen zu den empfohlenen Einstellungen zu Device Control entnehmen Sie bitte der *Richtlinienanleitung* zu Sophos Enterprise Console.

Hinweis: Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie konfigurieren zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

7.6.2 Device Control-Ereignisse

Device Control-Ereignisse (z.B. Sperren eines Wechselsmediums) werden im Dialogfeld **Device Control – Ereignisanzeige** angezeigt.

Im Dialogfeld **Device Control – Ereignisanzeige** können Sie Filter anlegen und sich nur Ereignisse anzeigen lassen, die für Sie relevant sind. Außerdem können Sie die Liste der Device Control-Ereignisse in eine Datei exportieren oder in die Zwischenablage kopieren. Nähere Informationen hierzu finden Sie unter *Anzeige von Device Control-Ereignissen* (Seite 213) und *Exportieren der Ereignisliste in eine Datei* (Seite 222).

Mit Device Control-Ereignissen können Sie bestimmte Geräte oder Gerätearten als Ausnahmen in die Device Control-Richtlinien aufnehmen. Nähere Informationen zum Erstellen von Ausnahmen für Geräte können Sie dem Abschnitt *Ausschließen von Geräten von einer einzelnen Richtlinie* (Seite 177) oder *Ausschließen eines Geräts von allen Richtlinien* (Seite 176) entnehmen.

Auf dem Dashboard wird die Anzahl der Computer angezeigt, auf denen die Summe der Device Control-Ereignisse in den vergangenen 7 Tagen den angegebenen Höchstwert überschritten hat. Nähere Informationen zum Festlegen des Höchstwerts finden Sie im Abschnitt *Konfigurieren des Dashboards* (Seite 56).

Zudem können Sie festlegen, dass die gewählten Empfänger über Device Control-Ereignisse benachrichtigt werden. Mehr dazu erfahren Sie unter *Einrichten von Device Control-Alerts und -Benachrichtigungen* (Seite 207).

7.6.3 Welche Geräte kann Device Control kontrollieren?

Mit Device Control können Sie drei Gerätetypen sperren: *Speicher*, *Netzwerk* und *kurze Reichweite*.

Speichermedien

- Wechselmedien (z.B. USB-Flash-Laufwerke, PC-Kartenlesegeräte und externe Festplatten)
- Optische Laufwerke (CD-ROM-/DVD-Laufwerke)
- Diskettenlaufwerke
- Sichere Wechselmedien (z.B. USB-Flash-Laufwerke mit Hardware-Verschlüsselung (SanDisk Cruzer Enterprise, SanDisk Cruzer Enterprise FIPS Edition, Kingston Data Traveler Vault – Privacy Edition, Kingston Data Traveler BlackBox und IronKey Enterprise Basic Edition)

Bei Bedarf können Sie auch unterstützte sichere Wechselmedien zulassen und andere Wechselmedien sperren. Eine aktuelle Liste der unterstützten sicheren Wechselmedien entnehmen Sie bitte dem Sophos Support-Artikel 63102 (*http://www.sophos.de/support/knowledgebase/article/63102.html*).

Netzwerkgeräte

- Modems
- Wireless-Geräte (Wi-Fi-Schnittstellen, 802.11-Standard)

Für Netzwerkschnittstellen können Sie zudem den Modus **Netzwerkbrücken sperren** auswählen, in dem das Risiko von Netzwerkbrücken zwischen einem Unternehmensnetzwerk und einem unternehmensfremden Netzwerk minimiert wird. Hierbei werden Wireless- oder Modemnetzwerkadapter deaktiviert, wenn ein Endpoint an ein physisches Netzwerk angeschlossen wird (in der Regel per Ethernet-Verbindung). Wenn der Endpoint von dem physischen Netzwerk getrennt wird, wird der Wireless- oder Modemnetzwerkadapter wieder aktiviert.

Kurze Reichweite

- Bluetooth-Schnittstellen
- Infrarot-Schnittstellen (IrDA)

Device Control sperrt interne und externe Geräte und Schnittstellen. Eine Richtlinie zum Sperren von Bluetooth blockiert beispielsweise:

- Die integrierte Bluetooth-Schnittstelle im Computer
- USB-Bluetooth-Adapter, die an den Computer angeschlossen werden.

7.6.4 Auswählen von Geräten für Device Control

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie bearbeiten zu können.

- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wichtig: Sie sollten keine Drahtlosverbindungen auf Computern trennen, die auf diese Weise über Enterprise Console verwaltet werden.

1. Prüfen Sie, welche Device Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Device Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Rufen Sie im Dialogfeld **Device Control-Richtlinie** die Registerkarte **Konfiguration** auf. Wählen Sie im Bereich **Speicher** das Speichermedium aus, das Sie steuern möchten.
4. Klicken Sie in der Spalte **Status** neben den Gerätetyp und öffnen Sie das Dropdown-Menü. Legen Sie eine Zugriffsart für die Geräte fest.

   Standardmäßig besitzen die Geräte Vollzugriff. Wechselmedien, optische Laufwerke und Diskettenlaufwerke können gesperrt oder mit Lesezugriff ausgestattet werden. Sichere Wechselmedien können gesperrt werden.

5. Wählen Sie im Bereich **Netzwerk** die Art des zu sperrenden Netzwerkgeräts aus.
6. Klicken Sie in der Spalte **Status** neben den Netzwerkgerätetyp und öffnen Sie das Dropdown-Menü.

   - Wählen Sie „Gesperrt“ aus, wenn der Gerätetyp gesperrt werden soll.
   - Wählen Sie „Netzwerkbrücken sperren“ aus, um Netzwerkbrücken zwischen einem Unternehmensnetzwerk und einem unternehmensfremden Netzwerk zu verhindern. Der Gerätetyp wird blockiert, wenn ein Endpoint an ein physisches Netzwerk angeschlossen wird (in der Regel über eine Ethernet-Verbindung). Wenn der Endpoint vom physischen Netzwerk abgetrennt wird, wird der Gerätetyp wieder aktiviert.

7. Wählen Sie im Bereich **Kurze Reichweite** den Gerätetyp mit kurzer Reichweite aus, der gesperrt werden soll. Wählen Sie in der Spalte **Status** neben dem Gerätetyp „Gesperrt“ aus.

   Klicken Sie auf **OK**.

7.6.5 Erkennen und Zulassen von Geräten

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können Geräte erkennen lassen, die jedoch nicht gesperrt werden sollen. Diese Option bietet sich an, wenn Sie Geräte künftig sperren möchten, erforderliche Geräte jedoch zunächst erkennen und zulassen möchten.

Wenn Sie Geräte erkennen, jedoch nicht sperren möchten, aktivieren Sie Device Control-Scans in einer Device Control-Richtlinie und aktivieren Sie den Modus *Nur Erkennen*. Ändern Sie den Status der zu erkennenden Geräte um in „Gesperrt“. Hierbei werden Ereignisse für Geräte auf Endpoints erstellt, wenn zwar Richtlinienverstöße vorliegen, die entsprechenden Geräte jedoch nicht gesperrt werden.

Nähere Informationen zur Anzeige von Device Control-Ereignissen finden Sie im Abschnitt *Anzeige von Device Control-Ereignissen* (Seite 213).

So können Sie Geräte anzeigen, ohne Sie zu sperren:

1. Prüfen Sie, welche Device Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Device Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Rufen Sie im Dialogfeld **Device Control-Richtlinie** die Registerkarte **Konfiguration** auf und wählen Sie die Option **Device Control-Scans aktivieren** aus.
4. Wählen Sie die Option **Geräte erkennen, aber nicht sperren**.
5. Sofern Sie dies nicht bereits erledigt haben, ändern Sie den Status der zu erkennenden Geräte um in „Gesperrt“. (Mehr dazu erfahren Sie unter *Auswählen von Geräten für Device Control* (Seite 173).)

   Klicken Sie auf **OK**.

7.6.6 Erkennen und Sperren von Geräten

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

1. Prüfen Sie, welche Device Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Device Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Rufen Sie im Dialogfeld **Device Control-Richtlinie** die Registerkarte **Konfiguration** auf und aktivieren Sie das Kontrollkästchen **Device Control-Scans aktivieren**.
4. Deaktivieren Sie die Option **Geräte erkennen, aber nicht sperren**.
5. Sofern Sie dies nicht bereits erledigt haben, ändern Sie den Status der zu sperrenden Geräte um in „Gesperrt“. (Mehr dazu erfahren Sie unter *Auswählen von Geräten für Device Control* (Seite 173).)

   Klicken Sie auf **OK**.

7.6.7 Ausschließen eines Geräts von allen Richtlinien

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können ein Gerät von allen Richtlinien, inklusive der Standardrichtlinie, ausschließen. Der Ausschluss wird dann zu allen neuen Richtlinien, die Sie erstellen, hinzugefügt.

Sie können ein einzelnes Gerät („nur dieses Gerät“) oder einen Gerätetyp („alle Geräte des Typs“) ausschließen. Schließen Sie nicht ein bestimmtes Gerät und den entsprechenden Gerätetyp gleichzeitig aus. Wenn Ausschlüsse für beides festgelegt werden, hat das Einzelgerät Vorrang.

So können Sie ein Gerät von allen Device Control-Richtlinien ausschließen:

1. Wählen Sie im Menü **Ereignisse** die Option **Device Control-Ereignisse**.

   Das Dialogfeld **Device Control – Ereignisanzeige** wird angezeigt.

2. Wenn nur ausgewählte Ereignisse angezeigt werden sollen, legen Sie im Feld **Suchkriterien** Filter fest und klicken Sie zur Anzeige der Ereignisse auf **Suchen**.

   Nähere Informationen finden Sie unter *Anzeige von Device Control-Ereignissen* (Seite 213).

3. Wählen Sie das Gerät aus, das von den Richtlinien ausgeschlossen werden soll und klicken Sie anschließend auf **Gerät ausschließen**.

   Das Dialogfeld **Gerät ausschließen** wird angezeigt. Im Bereich **Geräte-Details** werden Typ, Modell und Kennung des Geräts angezeigt. Im Bereich **Ausschluss-Details**, **Bereich** wird der Text „Alle Richtlinien.“ angezeigt.

   Hinweis: Wenn keine Ereignisse für das Gerät, das ausgeschlossen werden soll, vorhanden sind, (z.B. ein internes CD-/DVD-Laufwerk eines Endpoints), gehen Sie zu dem Computer mit dem Gerät und aktivieren Sie das Gerät im Geräte-Manager. (Rechtsklicken Sie zum Aufrufen des Geräte-Managers auf **Arbeitsplatz**, **Verwalten** und anschließend auf **Geräte-Manager**.) Im Dialogfeld **Device Control – Ereignisanzeige** wird ein neues „Sperr“-Ereignis angezeigt. Sie können das Gerät anhand der Anweisungen oben ausschließen.

4. Sie können auswählen, ob Sie nur dieses Gerät oder alle Geräte dieses Typs ausschließen möchten.
5. Weisen Sie dem Gerät Vollzugriff oder Lesezugriff zu.
6. Geben Sie in das Feld **Bemerkung** bei Bedarf einen Kommentar ein. So können Sie etwa angeben, wer den Geräteausschluss beantragt hat.
7. Klicken Sie auf **OK**.

7.6.8 Ausschließen von Geräten von einer einzelnen Richtlinie

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können bestimmte Geräte von einer Device Control-Richtlinie ausschließen.

Sie können ein einzelnes Gerät („nur dieses Gerät“) oder einen Gerätetyp („alle Geräte des Typs“) ausschließen. Schließen Sie nicht ein bestimmtes Gerät und den entsprechenden Gerätetyp gleichzeitig aus. Wenn Ausschlüsse für beides festgelegt werden, hat das Einzelgerät Vorrang.

So können Sie ein Gerät von einer Richtlinie ausschließen:

1. Prüfen Sie, welche Device Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Device Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Rufen Sie im Dialogfeld **Device Control-Richtlinie** die Registerkarte **Konfiguration** auf und klicken Sie auf **Ausschluss hinzu**.

   Das Dialogfeld **Device Control – Ereignisanzeige** wird angezeigt.
4. Wenn nur ausgewählte Ereignisse angezeigt werden sollen, legen Sie im Feld **Suchkriterien** Filter fest und klicken Sie zur Anzeige der Ereignisse auf **Suchen**.

   Nähere Informationen finden Sie unter *Anzeige von Device Control-Ereignissen* (Seite 213).
5. Wählen Sie das Gerät aus, das von der Richtlinie ausgeschlossen werden soll, und klicken Sie anschließend auf **Gerät ausschließen**.

   Das Dialogfeld **Gerät ausschließen** wird angezeigt. Im Bereich **Geräte-Details** werden Typ, Modell und Kennung des Geräts angezeigt. Im Bereich **Ausschluss-Details**, **Bereich** wird der Text „Nur diese Richtlinie.“ angezeigt.

   Hinweis: Wenn keine Ereignisse für das Gerät, das ausgeschlossen werden soll, vorhanden sind, (z.B. ein internes CD-/DVD-Laufwerk eines Endpoints), gehen Sie zu dem Computer mit dem Gerät und aktivieren Sie das Gerät im Geräte-Manager. (Rechtsklicken Sie zum Aufrufen des Geräte-Managers auf **Arbeitsplatz**, **Verwalten** und anschließend auf **Geräte-Manager**.) Im Dialogfeld **Device Control – Ereignisanzeige** wird ein neues „Sperr“-Ereignis angezeigt. Sie können das Gerät anhand der Anweisungen oben ausschließen.
6. Sie können auswählen, ob Sie nur dieses Gerät oder alle Geräte dieses Typs ausschließen möchten.
7. Weisen Sie dem Gerät Vollzugriff oder Lesezugriff zu.

8. Geben Sie in das Feld **Bemerkung** bei Bedarf einen Kommentar ein. So können Sie etwa angeben, wer den Geräteausschluss beantragt hat.
9. Klicken Sie auf **OK**.

7.6.9 Anzeigen/Ändern der Liste der ausgeschlossenen Geräte

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So können Sie sich die Liste der ausgeschlossenen Geräte anzeigen lassen:

1. Prüfen Sie, welche Device Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Device Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie im Dialogfeld **Device Control-Richtlinie** auf der Registerkarte **Konfiguration** den Gerätetyp aus, für den Ausschlüsse festgelegt werden sollen (z.B. optisches Laufwerk). Klicken Sie auf **Ausschlüsse anzeigen**.

   Das Dialogfeld <**Gerätetyp**> **Ausschlüsse** wird angezeigt. Wenn ein Ausschluss für alle Geräte des Modells angezeigt wird, ist das Feld **Geräte-ID** leer.
4. Verfahren Sie zum Bearbeiten der Liste ausgeschlossener Geräte wie folgt:
   - Wenn Sie einen Ausschluss hinzufügen möchten, klicken Sie auf **Hinzufügen**. Nähere Informationen finden Sie unter *Ausschließen von Geräten von einer einzelnen Richtlinie* (Seite 177).
   - Wenn Sie einen Ausschluss bearbeiten möchten, wählen Sie den Ausschluss aus, und klicken Sie auf **Ändern**. Ändern Sie die Einstellungen im Dialogfeld **Gerät ausschließen** nach Belieben.
   - Wenn Sie einen Ausschluss entfernen möchten, wählen Sie das entsprechende Gerät aus und klicken Sie auf **Entfernen**.

     Dadurch wird das ausgeschlossene Gerät aus der Richtlinie entfernt, die Sie ändern. Wenn Sie das Gerät aus weiteren Richtlinien entfernen möchten, wiederholen Sie die genannten Schritte für alle Richtlinien.

7.7 Konfigurieren der Richtlinie zur Festplattenverschlüsselung

7.7.1 Informationen zur Festplattenverschlüsselung

Hinweis: Die Funktion ist nicht im Umfang aller Lizenzen enthalten. Wenn Sie die Funktion nutzen möchten, müssen Sie eine entsprechende Lizenz erwerben. Nähere Informationen finden Sie unter *http://www.sophos.com/de-de/products/complete/comparison.aspx*.

Die Festplattenverschlüsselung schützt Daten auf Endpoints davor, von nicht autorisierten Personen gelesen oder geändert zu werden. Die Volumes auf den Festplatten sind transparent verschlüsselt. Die Benutzer müssen nicht entscheiden, welche Daten verschlüsselt werden sollen. Verschlüsselung und Entschlüsselung werden im Hintergrund ausgeführt.

Bei Computern mit Festplattenverschlüsselung wird die die Power-on Authentication (POA) vor dem Betriebssystem gestartet. Erst wenn sich der Benutzer an der POA angemeldet hat, wird das Betriebssystem gestartet und der Benutzer wird an Windows angemeldet.

Zur Unterstützung bei der Durchführung von IT-Aufgaben auf den Endpoints bietet die Festplattenverschlüsselung folgende Funktionen:

- Die Power-on Authentication lässt sich zur Benutzung mit Wake-on LAN vorübergehend deaktivieren. Dies erleichtert zum Beispiel die Verwaltung von Patches.
- In der Regel wird die POA von dem Benutzer aktiviert, der sich als erstes nach der Installation der Verschlüsselungssoftware am Endpoint anmeldet. Sie können Windows-Konten zur Anmeldung an Endpoints ohne Aktivierung der POA konfigurieren. Dies erleichtert die Arbeit von Mitarbeitern der IT-Abteilung, wie etwa Rollout-Beauftragten. Mit den in der Richtlinie zur Festplattenverschlüsselung als POA-Ausnahmen definierten Windows-Konten können sie sich zu Installations- und Prüfungszwecken an neuen Computern anmelden. Im Anschluss melden sich dann die Endbenutzer an und aktivieren die POA.
- Sie können POA-Benutzerkonten so konfigurieren, dass sich Mitglieder der IT-Abteilung bei bereits aktiver POA an Endpoints anmelden und administrative Aufgaben ausführen können.

Die Wiederherstellung von Computern mit Festplattenverschlüsselung erfolgt anhand der folgenden Methoden:

- **Challenge/Response** hilft Benutzern, die sich nicht an ihrem Computer anmelden oder nicht auf verschlüsselte Daten zugreifen können. Für das Challenge/Response-Verfahren ist die Unterstützung des Helpdesks erforderlich. Während eines Challenge/Response-Vorgangs übermittelt der Benutzer einen auf dem Endpoint-Computer erzeugten Challenge-Code an den Helpdesk-Beauftragten. Der Helpdesk-Beauftragte erzeugt einen Response-Code, der den Benutzer zum Ausführen einer bestimmten Aktion auf dem Computer berechtigt.
- Mit Local Self Help können sich Benutzer, die ihr Kennwort vergessen haben, ohne Unterstützung des Helpdesks an ihrem Computer anmelden. Benutzer beantworten bei der Anmeldung vordefinierte Fragen in der Power-on Authentication. Local Self Help reduziert die Anzahl an Helpdesk-Anfragen. Helpdesk-Mitarbeiter können sich so auf komplexere Support-Aufgaben konzentrieren.

Nähere Informationen zu den empfohlenen Einstellungen zur Festplattenverschlüsselung entnehmen Sie bitte der *Richtlinienanleitung* zu *Sophos Endpoint Security and Control*.

7.7.2 Konfigurieren der Festplattenverschlüsselung

Warnhinweis: Bei der Erstinstallation von Sophos Verschlüsselungssoftware empfiehlt sich, alle Einstellungen schrittweise zu aktivieren und zu testen.

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Festplattenverschlüsselung** verfügen, um eine Richtlinie zur Festplattenverschlüsselung bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Die Festplattenverschlüsselung ist standardmäßig nicht aktiviert.
So aktivieren und konfigurieren Sie die Festplattenverschlüsselung:

1. Prüfen Sie, welche Richtlinie zur Festplattenverschlüsselung von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Festplattenverschlüsselung**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Festplattenverschlüsselung** wird angezeigt.

3. Geben Sie im Bereich **Zu verschlüsselnde Laufwerke** durch Auswahl der entsprechenden Optionen an, welche Volumes verschlüsselt werden sollen:

   - **Boot-Laufwerke**
   - **Keine Boot-Laufwerke**

4. Wählen Sie **Schnelle Erstverschlüsselung (nur genutzte Festplattenbereiche werden verschlüsselt)**, um die Dauer der Erstverschlüsselung zu reduzieren.

   Hinweis: Wenn eine Festplatte vor der Verschlüsselung verwendet wurde, ist die schnelle Erstverschlüsselung unter Umständen unsicherer. Nicht verwendete Sektoren können noch Daten enthalten.

5. Klicken Sie auf **OK**.

Wenn Sie die Richtlinie zur Festplattenverschlüsselung mit diesen Einstellungen auf eine Computergruppe mit der aktuellen Verschlüsselungssoftware von Sophos übertragen, wird der Verschlüsselungsvorgang eingeleitet, wenn die Richtlinie abgerufen wurde. Der Benutzer muss seine Arbeit nicht unterbrechen.

Hinweis: Zum Entschlüsseln der Computer deaktivieren Sie die entsprechenden Optionen unter **zu verschlüsselnde Volumes** und weisen Sie die Richtlinie den zu entschlüsselnden Computern zu. Benutzer können die entsprechenden Laufwerke dann manuell entschlüsseln.

7.7.3 Konfiguration der Anmeldung

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Festplattenverschlüsselung** verfügen, um eine Richtlinie zur Festplattenverschlüsselung bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Standardmäßig werden Computer mit einer Richtlinie zur Festplattenverschlüsselung von der POA geschützt.
So können Sie die Anmeldung an der POA auf den Benutzercomputern konfigurieren:

1. Prüfen Sie, welche Richtlinie zur Festplattenverschlüsselung von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Festplattenverschlüsselung**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Festplattenverschlüsselung** wird angezeigt.

3. Gehen Sie zur **Power-on Authentication (POA)**.
4. Vergewissern Sie sich, dass **Power-on Authentication (POA) aktivieren** aktiviert ist.

   Des Weiteren können Sie Windows-Konten zur Anmeldung an Endpoints zur Ausführung von Aufgaben nach der Installation ohne Aktivierung der POA konfigurieren.

   a) Klicken Sie auf die Schaltfläche **Ausnahmen** neben dem Feld **Power-on Authentication (POA) aktivieren**.

      Das Dialogfeld **Ausnahmen** wird angezeigt.

   b) Klicken Sie auf **Hinzufügen**, geben Sie den **Benutzernamen** und den **Computer- oder Domänennamen** der/des Windows-Kontos/Konten ein und klicken Sie auf **OK**.

      Hinweis: In den Feldern **Benutzername** und **Computer- oder Domänenname** kann das erste oder letzte Zeichen durch einen Platzhalter ersetzt werden. Im Feld **Benutzername** ist das ? nicht zulässig. Im Feld **Computer- oder Domänenname** sind die Zeichen / \ [ ] : ; | = , + ? < > " nicht zulässig.

5. Wählen Sie **Fingerabdruck**, damit sich Benutzer mit dem Lenovo Fingerabdruck-Leser anmelden können.
6. Wenn Sie einen Benutzer angeben möchten, der sich bei bereits aktiver POA am Endpoint anmelden und administrative Aufgaben durchführen kann, wählen Sie **POA-Benutzer** und klicken Sie auf die Schaltfläche **Konfigurieren**.

   a) Geben Sie im Dialogfeld **POA-Benutzer konfigurieren** einen Anmeldenamen für den POA-Benutzer in das Feld **Benutzername** ein. Sie können den Anmeldenamen frei wählen, sofern die folgende Ausnahmen beachtet werden:

      Hinweis: Im Feld **Benutzername** sind die Zeichen / \ [ ] : ; | = , + ? < > " * nicht zulässig.

Hinweis: Bei der Einrichtung und Eingabe des Anmeldenamens für POA-Benutzer auf Japanisch müssen die Zeichen in Romaji (lateinischer Schrift) angegeben werden, damit die Anmeldung an der POA erfolgreich ist.

b) Klicken Sie auf die Schaltfläche **Festlegen** neben dem Feld **Kennwort**.

Das Dialogfeld **POA-Benutzerkennwort** wird angezeigt.

c) Geben Sie ein Kennwort zum POA-Benutzernamen ein, wiederholen Sie die Eingabe und klicken Sie auf **OK**.

Hinweis: Bei der Einrichtung und Eingabe von Kennwörtern für POA-Benutzer auf Japanisch müssen die Zeichen in Romaji (lateinischer Schrift) angegeben werden, damit die Anmeldung an der POA erfolgreich ist.

d) Klicken Sie im Fenster **POA-Benutzer konfigurieren** auf **OK**.

7. Wenn Sie die vorübergehende Deaktivierung der POA für Wake-on LAN konfigurieren möchten, wählen Sie **Vorübergehende Deaktivierung der POA (für Wake-on LAN)**.

   Weitere Informationen finden Sie unter *Konfigurieren der vorübergehenden Deaktivierung der POA für Wake-on LAN* (Seite 182).

8. Klicken Sie im Dialogfeld **Festplattenverschlüsselung** auf **OK**.

Hinweis: Wenn Sie die Option **Power-on Authentication (POA) aktivieren** ausgewählt haben, werden Sie zur Bestätigung der Deaktivierung der POA aufgefordert. Aus Sicherheitsgründen wird von der Deaktivierung der POA abgeraten. Durch Deaktivierung der POA reduziert sich die Systemsicherheit auf den Schutz durch die Windows-Anmeldung. Dadurch erhöht sich das Risiko des unberechtigten Zugriffs auf verschlüsselte Daten.

7.7.4 Konfigurieren der vorübergehenden Deaktivierung der POA für Wake-on LAN

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Festplattenverschlüsselung** verfügen, um eine Verschlüsselungsrichtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.
- In der Verschlüsselungsrichtlinie muss die Option **Power-on Authentication (POA) aktivieren** ausgewählt werden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Standardmäßig werden Computer mit Festplattenverschlüsselung von der POA geschützt. Die Power-on Authentication lässt sich zur Benutzung mit Wake-on LAN vorübergehend deaktivieren. Dies erleichtert zum Beispiel die Verwaltung von Patches. Wake-on LAN wird durch Ausführen des Zeitsteuerungs-Skripts "SGMCMDIntn.exe" auf dem Endpoint ausgeführt.

Hinweis: Wir weisen an dieser Stelle ausdrücklich darauf hin, dass auch das zeitlich begrenzte „Ausschalten“ der POA für eine bestimmte Anzahl von Boot-Vorgängen ein Absenken des Sicherheitsniveaus bedeutet.

1. Prüfen Sie, welche Verschlüsselungsrichtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Festplattenverschlüsselung**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Festplattenverschlüsselung** wird angezeigt.

3. Stellen Sie im Bereich **Power-on Authentication (POA)** sicher, dass die Option **Power-on Authentication (POA) aktivieren** aktiviert ist.
4. Wählen Sie **Vorübergehende Deaktivierung (für Wake-on LAN)** und klicken Sie auf **Konfigurieren**.

   Das Dialogfeld **Vorübergehende Deaktivierung konfigurieren** wird angezeigt.

5. Geben Sie in den Feldern **Start** und **Ende** den Start- und Endzeitpunkt für den Wake-on LAN-Vorgang an.
6. Wählen Sie die Option **Windows-Anmeldung in dem Zeitraum zulassen**, um die Windows-Anmeldung bei Wake-on LAN (zum Beispiel zum Download von Software-Updates) zu gestatten.
7. Geben Sie im Feld **Automatische Anmeldungsbeschränkung** an, wie oft der Computer während des Wake-on LAN-Vorgangsohne Authentifizierung über die POA neu gestartet werden darf.

   Hinweis: Es empfiehlt sich, für alle Eventualitäten drei Neustarts mehr zu erlauben.

8. Klicken Sie auf **OK**.

7.7.4.1 Beispiel für Wake-on LAN

Bei einem Software-Rollout, das zwischen 03.00 Uhr und 06.00 Uhr an einem bestimmten Tag stattfinden soll, sind zwei Neustarts erforderlich. Der lokale Software-Rollout-Agent muss sich an Windows anmelden können.

In der Richtlinie zur Festplattenverschlüsselung können Sie im Bereich **Vorübergehende Deaktivierung (für Wake-on LAN)** folgende Einstellungen konfigurieren:

Richtlinieneinstellung	Wert
Start	Tag vor dem Rollout, 12.00 Uhr
Ende	Tag des Rollouts, 6.00 Uhr
Windows-Anmeldung in dem Zeitraum zulassen	Ja
Automatische Anmeldungsbeschränkung	5

Da die Höchstanzahl an automatischen Anmeldungen 5 beträgt, startet der Endpoint 5 Mal ohne Authentifizierung durch die POA.

Hinweis: Im vorliegenden Beispiel sind die automatischen Anmeldungen auf 5 beschränkt, da sich empfiehlt, drei weitere Neustarts zuzulassen.

Wenn Sie die Startzeit auf 12.00 Uhr am Tag des Software-Rollout legen, wird das Zeitsteuerungs-Skript „SGMCMDIntn.exe“ rechtzeitig gestartet und der Wake-on LAN-Vorgang wird nicht vor 03.00 Uhr am Tag des Rollouts eingeleitet.

Das Software-Rollout-Team muss die folgenden Befehle zur Erstellung des Zeitsteuerungs-Skripts „SGMCMDIntn.exe“ generieren:

- Start am Tag vor dem Software-Rollout, 12.15 Uhr, SGMCMDIntn.exe -WOLstart
- Start am Tag nach dem Software-Rollout, 09.00 Uhr, SGMCMDIntn.exe -WOLstop

Der Zeitpunkt des Software-Rollout-Skripts wird als Tag des Rollouts, 03.00 Uhr definiert. Wake-on LAN kann am Ende des Skripts über „SGMCMDIntn.exe -WOLstop“ deaktiviert werden.

Alle Endpoints, die sich bis zum **Startzeitpunkt** anmelden und eine Verbindung zu den Roll-out Servern in Verbindung herstellen, erhalten die neue Richtlinie und die Zeitsteuerungsbefehle.

Endpoints, auf denen die Zeitsteuerung den Befehl „SGMMCMDIntn -WOLStart“ zwischen 12.00 Uhr am Tag vor dem Rollout und 06.00 Uhr am Tag des Rollouts auslöst, fallen in den WOL-Zeitraum. Wake-on LAN wird also aktiviert.

7.7.5 Konfiguration von Challenge/Response

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Festplattenverschlüsselung** verfügen, um eine Verschlüsselungsrichtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.
- In der Verschlüsselungsrichtlinie muss die Option **Power-on Authentication (POA) aktivieren** ausgewählt werden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Challenge/Response hilft Benutzern, die sich nicht an ihrem Computer anmelden oder nicht auf verschlüsselte Daten zugreifen können. Für das Challenge/Response-Verfahren ist die Unterstützung des Helpdesks erforderlich.

So konfigurieren Sie Challenge/Response:

1. Prüfen Sie, welche Verschlüsselungsrichtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Festplattenverschlüsselung**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Festplattenverschlüsselung** wird angezeigt.

3. Stellen Sie im Bereich **Power-on Authentication (POA)** sicher, dass die Option **Power-on Authentication (POA) aktivieren** aktiviert ist.
4. Stellen Sie im Bereich **Methoden zum Recovery für die Anmeldung** sicher, dass **Challenge/Response (Helpdesk erforderlich)** ausgewählt wurde.
5. Klicken Sie auf **Konfigurieren** neben **Challenge/Response (Helpdesk erforderlich)**.

   Das Dialogfeld **Willkommenstext für Challenge/Response konfigurieren** wird angezeigt.

6. Ein Textfeld wird angezeigt. Sie können den Text eingeben, der angzeigt wird, wenn der Benutzer ein Challenge/Response-Verfahren in der POA einleitet. Beispiel: „Bitte rufen Sie Ihren Support unter der Telefonnummer 1234-56789 an.“). Klicken Sie nach Eingabe des Texts auf **OK**.
7. Klicken Sie auf **OK**.

7.7.6 Konfigurieren der Local Self Help

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Festplattenverschlüsselung** verfügen, um eine Verschlüsselungsrichtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.
- Zu Konfiguration der globalen Einstellungen von Local Self Help müssen Sie über die Berechtigung **Globale Verschlüsselungseinstellungen** verfügen.
- In der Verschlüsselungsrichtlinie muss die Option **Power-on Authentication (POA) aktivieren** ausgewählt werden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Mit Local Self Help können sich Benutzer, die ihr Kennwort vergessen haben, ohne Unterstützung des Helpdesks an ihrem Computer anmelden. Benutzer beantworten bei der Anmeldung vordefinierte Fragen in der Power-on Authentication.

So konfigurieren Sie Local Self Help:

1. Prüfen Sie, welche Verschlüsselungsrichtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Festplattenverschlüsselung**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Festplattenverschlüsselung** wird angezeigt.

3. Stellen Sie im Bereich **Power-on Authentication (POA)** sicher, dass die Option **Power-on Authentication (POA) aktivieren** aktiviert ist.

4. Wählen Sie im Bereich **Methoden zum Recovery für die Anmeldung** die Option **Local Self Help (ohne Helpdesk)** und klicken Sie auf **OK**.
5. Wenn Sie weitere Einstellungen der Local Self Help konfigurieren möchten, klicken Sie auf **Globale Verschlüsselungseinstellungen**.

   Das Dialogfeld **Globale Verschlüsselungseinstellungen** wird angezeigt.

6. Konfigurieren Sie unter **Local Self Help** die folgenden Einstellungen:

   a) Geben Sie im Dropdown-Menü **Der Benutzer muss Folgendes beantworten:** an, wie viele Fragen der Benutzer richtig beantworten muss.

   b) Um die Benutzer dazu zu berechtigen, eigene Fragen zu definieren, wählen Sie **Benutzer dürfen eigene Fragen festlegen**.

7. Klicken Sie auf **OK**.

7.7.7 Konfiguration der globalen Verschlüsselungseinstellungen

Bei rollenbasierter Verwaltung müssen Sie über die Berechtigung **Globale Verschlüsselungseinstellungen** verfügen.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Neben der Richtlinien zur Festplattenverschlüsselung können Sie zudem die folgenden globalen Verschlüsselungseinstellungen konfigurieren: Anzeigeeinstellungen, globale Einstellungen für Local Self Help und Protokolleinstellungen.
So konfigurieren Sie die globalen Verschlüsselungseinstellungen:

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Festplattenverschlüsselung**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Festplattenverschlüsselung** wird angezeigt.

2. Klicken Sie auf **Globale Verschlüsselungseinstellungen**.

   Das Dialogfeld **Globale Verschlüsselungseinstellungen** wird angezeigt.

3. Konfigurieren Sie unter **Anzeige** die folgenden Einstellungen:

   a) Wenn das Symbol der Festplattenverschlüsselung für schnelleren Zugriff auf die Funktionen im Infobereich von Windows auf den Endpoints angezeigt werden soll, wählen Sie **Symbol im Infobereich in Windows**.

   b) Zur Anzeige des Verschlüsselungsymbols in Windows Explorer auf Endpoints für verschlüsselte Laufwerke, wählen Sie **Verschlüsselungsstatus in Windows Explorer**.

   c) Zur Anzeige des gewünschten Texts bei der Anmeldung an der POA wählen Sie **Rechtliche Hinweise beim Starten des Computers**. Zur Konfiguration des Anzeigetexts (zum Beispiel rechtliche Hinweise, die aus rechtlichen Gründen angezeigt werden müssen, oder Informationen für Personen, die ein Laptop auffinden) klicken Sie auf **Konfigurieren**, geben Sie den gewünschten Text in das Dialogfeld **Rechtliche Hinweise konfigurieren** ein und klicken Sie auf **OK**.

4. Im Bereich **Local Self Help** können Sie globale Einstellungen für die Local Self Help für Recovery für die Anmeldung festlegen. Weitere Informationen finden Sie unter *Konfigurieren der Local Self Help* (Seite 185).
5. Klicken Sie auf **OK**.

7.7.8 Sichern von Unternehmenszertifikaten

Bei rollenbasierter Verwaltung müssen Sie über die Berechtigung **Globale Verschlüsselungseinstellungen** verfügen.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Zertifikate dienen der Absicherung der Kommunikation zwischen Endpoint und Datenbank. Wenn Verschlüsselung installiert wird, wird eine beschädigte Datenbank mit dem Unternehmenszertifikat wiederhergestellt. Das Unternehmenszertifikat wird im Zuge der Installation von Enterprise Console gesichert. Sie können jedoch jederzeit an anderen Orten ein Backup erstellen.

Hinweis: Ein weiteres Zertifikat ist das MSO-Zertifikat. Das Zertifikat dient der Wiederherstellung beschädigter Server. Das MSO-Zertifikat kann nur im Zuge der Installation von Enterprise Console gesichert werden. Stellen Sie sicher, dass Sie das Backup nicht verlieren.

So sichern Sie das Unternehmenszertifikat:

1. Klicken Sie im Menü **Extras** auf **Verschlüsselung verwalten** und wählen Sie **Unternehmenszertifikat sichern**.
2. Klicken Sie im Bereich **Unternehmenszertifikat sichern** auf **Exportieren**.
3. Wählen Sie einen Speicherort für das Backup, geben Sie Ihr Kennwort ein und bestätigen Sie die Eingabe, um die Sicherung zu verschlüsseln. Notieren Sie sich das Kennwort.

7.8 Konfigurieren der Manipulationsschutz-Richtlinie

7.8.1 Allgemeine Informationen

Mit dem Manipulationsschutz können Sie verhindern, dass nicht autorisierte Benutzer (lokale Administratoren und Benutzer ohne hinreichende Fachkenntnisse) und bekannte Malware Sophos Sicherheitssoftware deinstallieren bzw. über Sophos Endpoint Security and Control deaktivieren.

Hinweis: Der Manipulationsschutz schützt nicht vor Benutzern mit ausgeprägtem Technikverständnis. Auch bietet die Funktion keinen Schutz vor Malware, die eigens dafür konzipiert wurde, das Betriebssystem zu untergraben und die Erkennung zu umgehen. Diese Malware-Art wird ausschließlich von Scans auf Threats und verdächtigem Verhalten erkannt. Weitere Informationen finden Sie unter *Die Antivirus- und HIPS-Richtlinie* (Seite 94).

Nach der Aktivierung des Manipulationsschutzes und der Erstellung eines Manipulationsschutz-Kennworts können Mitglieder der Gruppe SophosAdministrators folgende Aktionen nur unter Angabe des Kennworts vornehmen:

- Erneute Konfiguration der Einstellungen von On-Access-Scans bzw. der Erkennung verdächtigen Verhaltens in Sophos Endpoint Security and Control.

- Deaktivieren des Manipulationsschutzes.
- Deinstallation von Komponenten von Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate oder Sophos Remote Management System).
- Deinstallation von Sophos Disk Encryption.

Wenn Sie möchten, dass SophosAdministrators diese Aufgaben ausführen können, müssen Sie den Administratoren das Manipulationsschutz-Kennwort zur Authentifizierung geben.

Der Manipulationsschutz betrifft Mitglieder der Gruppe SophosUsers und SophosPowerUsers nicht. Auch bei aktiviertem Manipulationsschutz können diese Benutzer weiterhin ohne Eingabe von Kennwörtern die Aufgaben ausführen, zu deren Ausführung sie berechtigt sind.

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Manipulationsschutz-Richtlinie ist die Berechtigung **Richtlinieneinstellung – Manipulationsschutz** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Manipulationsschutz-Ereignisse

Manipulationsschutz-Ereignisse (z.B. der unbefugte Versuch, Sophos Anti-Virus von einem Endpoint zu entfernen, wurde unterbunden) werden im Ereignisprotokoll festgehalten und können mit Enterprise Console angezeigt werden. Mehr dazu erfahren Sie unter *Anzeige von Manipulationsschutz-Ereignissen* (Seite 216).

Es wird zwischen den folgenden Manipulationsschutz-Ereignissen unterschieden:

- Erfolgreiche Manipulationsschutz-Ereignisse (Anzeige des Namens des authentifizierten Benutzers sowie des Authentifizierungszeitpunkts).
- Nicht erfolgreiche Manipulationsschutz-Ereignisse (Anzeige des Zielprodukts/der Zielkomponente, des Manipulationszeitpunkts und der Daten des Benutzers, der den Manipulationsversuch unternommen hat).

7.8.2 Aktivieren/Deaktivieren des Manipulationsschutzes

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Manipulationsschutz-Richtlinie ist die Berechtigung **Richtlinieneinstellung – Manipulationsschutz** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So aktivieren/deaktivieren Sie den Manipulationsschutz:

1. Prüfen Sie, welche Manipulationsschutz-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Bereich **Richtlinien** auf **Manipulationsschutz**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Wählen Sie im Dialogfeld **Manipulationsschutz-Richtlinie** das Kontrollkästchen **Manipulationsschutz aktivieren** aus bzw. ab.

   Wenn Sie den Manipulationsschutz zum ersten Mal aktivieren, klicken Sie auf **Festlegen** unter dem Feld **Kennwort**. Geben Sie das Kennwort in das Feld **Manipulationsschutz-Kennwort** ein und bestätigen Sie es.

   Tipp: Das Kennwort sollte mindestens 8 Zeichen umfassen und sich aus Buchstaben und Zahlen zusammensetzen.

7.8.3 Ändern des Manipulationsschutz-Kennworts

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Manipulationsschutz-Richtlinie ist die Berechtigung **Richtlinieneinstellung – Manipulationsschutz** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So ändern Sie das Manipulationsschutz-Kennwort:

1. Prüfen Sie, welche Manipulationsschutz-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Bereich **Richtlinien** auf **Manipulationsschutz**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Manipulationsschutz-Richtlinie** unter dem Feld **Kennwort** auf **Ändern**. Geben Sie in das Feld **Manipulationsschutz-Kennwort** ein Kennwort ein und bestätigen Sie es.

   Tipp: Das Kennwort sollte mindestens 8 Zeichen umfassen und sich aus Buchstaben und Zahlen zusammensetzen.

7.9 Konfigurieren der Patch-Richtlinie

7.9.1 Informationen zur Patch-Analyse

Hinweis: Die Funktion ist nicht im Umfang aller Lizenzen enthalten. Wenn Sie die Funktion nutzen möchten, müssen Sie eine entsprechende Lizenz erwerben. Nähere Informationen finden Sie unter *http://www.sophos.com/de-de/products/complete/comparison.aspx*.

Mit Enterprise Console wird festgestellt, ob die aktuellen Sicherheits-Patches auf den Computern installiert wurden.

Anhand der von den SophosLabs bereitgestellten Bewertung können Sie ermitteln, welche Sicherheits-Patch-Probleme das höchste Risiko bergen, und diese umgehend beheben. Die Bewertungen der SophosLabs basieren auf den aktuellen Exploits und weichen daher unter Umständen vom vom Hersteller angegebenen Schweregrad ab.

Wenn Sie die Patch-Analyse nutzen möchten, muss zunächst der Patch Agent auf allen Computern im Netzwerk installiert sein, damit der Patch-Status ermittelt und an Enterprise Console übertragen werden kann. Den Agenten können Sie über den **Assistenten zum Schutz von Computern** installieren. Mehr dazu erfahren Sie unter *Automatisches Schützen von Computern* (Seite 51).

Hier wird davon ausgegangen, dass Sie den Patch Agent installiert haben.

Hinweis: Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Patch-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Patch** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 17) entnehmen.

7.9.2 Funktionsweise der Patch-Analyse

Die Patch-Analyse ist in der Standardrichtlinie deaktiviert. Nach der Aktivierung der Patch-Analyse leiten die Computer die Analyse ein. Dies kann einige Minuten dauern. Weitere Prüfungen erfolgen in den in der Richtlinie festgelegten Zeitabständen (das Standard-Intervall lautet „täglich“).

Hinweis: Wenn die Computer die Analyse durchführen, bevor Enterprise Console zum ersten Mal Patch-Daten von Sophos heruntergeladen hat, werden keine Ereignisse in der Patch-Ereignisanzeige angezeigt. Der Download kann mehrere Stunden in Anspruch nehmen. Im Feld **Patch-Updates** unter **Patch-Ereignisse** > **Patch-Analyse-Ereignisse** können Sie überprüfen, ob der Vorgang abgeschlossen wurde.

Wenn der Patch Agent keine Updates von Enterprise Console beziehen kann, werden Computer weiterhin mit den zuvor heruntergeladenen Patch-Erkennungen abgeglichen.

Computer werden lediglich auf die Sicherheits-Patches für auf dem Computer installierte Software überprüft. Wenn ein neuer Patch veröffentlicht wird, der einen älteren Patch ablöst,

überprüft die Patch-Analyse nicht mehr, ob ältere Patches vorhanden sind. Die Analyse basiert nur auf dem neuen Patch.

Sie können Sophos NAC so konfigurieren, dass auf der Basis der Patch-Ergebnisse entschieden wird, ob ein Computer auf das Netzwerk zugreifen darf.

7.9.2.1 Abgelöste Patches

Wenn ein Hersteller einen neuen Patch veröffentlicht, der einen älteren Patch ablöst, handelt es sich bei dem neuen Patch um den ablösenden Patch. Der ersetzte Patch wird als abgelöster Patch bezeichnet.

Es empfiehlt sich, den ablösenden Patch zu installieren, um die Computer auf dem neuesten Stand zu halten.

Beispiel: Wenn Sie nach VirusX suchen und feststellen, dass der Virus in Patch P01 enthalten ist, der von Patch P02 abgelöst wurde, empfiehlt sich, P02 zu installieren.

7.9.3 Patch-Analyse-Ereignisse

Patch-Analyse-Ereignisse (z.B. fehlender Patch auf einem Computer) werden in der **Patch-Analyse – Ereignisanzeige** angezeigt.

In der **Patch-Analyse – Ereignisanzeige** können Sie Filter anlegen und sich nur Ereignisse anzeigen lassen, die für Sie relevant sind. Außerdem können Sie die Liste der Patch-Analyse-Ereignisse in eine Datei exportieren oder in die Zwischenablage kopieren. Nähere Informationen hierzu finden Sie unter *Anzeige der Patch-Analyse-Ereignisse* (Seite 217) und *Exportieren der Ereignisliste in eine Datei* (Seite 222).

7.9.4 Aktivieren/Deaktivieren der Patch-Analyse

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Patch-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Patch** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So aktivieren/deaktivieren Sie die Patch-Analyse:

1. Überprüfen Sie, welche Patch-Richtlinie den zu konfigurierenden Computern zugewiesen wurde.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Patch**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Deaktivieren Sie im Dialogfeld **Patch-Richtlinie** das Kontrollkästchen **Patch-Analyse aktivieren** und klicken Sie auf **OK**.

7.9.5 Auswahl des Intervalls für die Patch-Analyse

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Patch-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellung – Patch** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So legen Sie das Patch-Intervall fest.

1. Überprüfen Sie, welche Patch-Richtlinie den zu konfigurierenden Computern zugewiesen wurde.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Patch**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Klicken Sie im Dialogfeld **Patch-Richtlinie** auf den Dropdown-Pfeil **Auf fehlende Patches überprüfen** und wählen Sie das gewünschte Intervall aus. Klicken Sie auf **OK**.

   Wenn Sie das Intervall übernehmen möchten, muss die Patch-Analyse in der Richtlinie aktiviert werden.

7.10 Konfigurieren der Web Control-Richtlinie

7.10.1 Informationen zur Web Control-Richtlinie

Hinweis: Die Funktion ist nicht im Umfang aller Lizenzen enthalten. Wenn Sie die Funktion nutzen möchten, müssen Sie eine entsprechende Lizenz erwerben. Nähere Informationen finden Sie unter *http://www.sophos.com/de-de/products/complete/comparison.aspx*.

Die Web Control-Richtlinie ist in Enterprise Console standardmäßig deaktiviert. Wenn Sie die Option **Web Control aktivieren** auswählen, stehen folgende Optionen zur Verfügung:

- **Kontrolle unangebrachter Websites**: Die Basisoption von Web Control umfasst 14 Website-Kategorien. Mit dieser Funktion kann verhindert werden, dass Benutzer unangebrachte Websites aufrufen und das Unternehmen strafrechtlich belangt wird. Weitere Informationen finden Sie unter *Informationen zur Kontrolle unangebrachter Websites* (Seite 193).
- **Vollständige Web Control**: Bei dieser Option wird eine umfassende Web-Richtlinie eingesetzt, die mit einer Sophos Web Appliance oder einer Security Management Appliance konfiguriert und bereitgestellt wird. Die umfassende Web-Richtlinie wird durchgesetzt. Zudem werden umfassende Reports zum Datenverkehr im Web erstellt. Für die Option ist eine Sophos Web Appliance oder eine Management Appliance erforderlich. Weitere Informationen finden Sie unter *Vollständige Web Control* (Seite 198).

Mit der Kontrolle potenziell unangebrachter Websites können Sie vorhandene Web Control-Richtlinien bearbeiten oder eine neue Richtlinie erstellen. Weitere Informationen

finden Sie unter *Erstellen einer Richtlinie* (Seite 35). Sie können den Website-Kategorien die Aktionen „blockieren“, „warnen“ oder „zulassen“ zuordnen. Der Web Control-Status und Web-Ereignisse werden in Enterprise Console angezeigt. Weitere Informationen zu Web-Ereignissen finden Sie unter *Anzeige von Web-Ereignissen* (Seite 220).

Wenn Sie die Vollständige Web Control-Richtlinie verwenden, benötigt Enterprise Console den Standort der Web Appliance oder der Management Appliance, mit der die Web-Filter-Richtlinie konfiguriert wird, sowie einen geteilten Schlüssel zur Absicherung der Kommunikation zwischen Appliance und Enterprise Console. Bei Auswahl der Vollständigen Web Control-Richtlinie erfolgen Reports und die Überwachung in der Web Appliance oder der Management Appliance. Websites werden jedoch von der URL-Live-Filterfunktion (Web-Schutz) in Sophos Endpoint Security and Control gescannt und analysiert, und Ergebnisse werden in Enterprise Console als Web-Ereignisse angezeigt.

Hinweis: Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Web Control** verfügen, um eine Web Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 17) entnehmen.

7.10.2 Kontrolle unangebrachter Websites

7.10.2.1 Informationen zur Kontrolle unangebrachter Websites

Hinweis: Die Funktion ist nicht im Umfang aller Lizenzen enthalten. Wenn Sie die Funktion nutzen möchten, müssen Sie eine entsprechende Lizenz erwerben. Nähere Informationen finden Sie unter *http://www.sophos.com/de-de/products/complete/comparison.aspx*.

Bei der Basisversion der Kontrolle von Websites können Sie die Aktivitäten der Benutzer anhand von 14 Kategorien filtern. Den Kategorien wurde jeweils eine Standardmaßnahme zugeordnet (Details können Sie dem Abschnitt *Website-Kategorien* (Seite 194) entnehmen). Sie können die Maßnahme jedoch auch nach Wunsch anpassen. Entsprechende Anweisungen entnehmen Sie bitte dem Abschnitt *Auswahl einer Maßnahme zu Website-Kategorien* (Seite 197).

Benutzern kann der Zugriff auf eingeschränkte Websites verweigert werden. Dem Benutzer wird ein Ereignis angezeigt, das ebenfalls an Enterprise Console übermittelt wird.

Benutzer können jedoch auch beim Aufrufen kontrollierter Websites gewarnt werden. Auch wenn der Benutzer den Fortgang nicht fortsetzt, wird die Warnung angezeigt. Ruft der Benutzer die Seite trotz der Warnmeldung auf, wird ein weiteres Ereignis an Enterprise Console gesendet.

Hinweis: Sowohl HTTP- als auch HTTPS-Websites werden zwar in allen unterstützten Browsern gefiltert, die Benutzerbenachrichtigungen unterscheiden sich jedoch. Bei HTTP-Seiten werden Benutzer über Seiten benachrichtigt, die in die Kategorie „Blockieren“ oder „Warnen“ fallen. Bei HTTPS werden Benutzer lediglich über Seiten aus der Kategorie „Blockieren“ in Form einer Sprechblasenmeldung in der Symbolleiste von Windows informiert. „Warn“-Maßnahmen werden bei HTTPS weder angezeigt noch blockiert. Benutzer können

die gewünschte Seite aufrufen. Das Ereignis wird in Enterprise Console als Maßnahme „Fortsetzen“ protokolliert.

Bei Auswahl der Maßnahme „Zulassen“ für eine Website-Kategorie können Benutzer alle Seiten in der Kategorie aufrufen, sofern keine Website-Ausschlüsse definiert wurden. Bei Auswahl der **Kontrolle unangebrachter Websites** werden Ereignisse in Zusammenhang mit der Maßnahme „Zulassen“ nicht protokolliert.

Hinweis: Zugelassene Websites werden dennoch von der Live-URL-Filterfunktion (Web-Schutz) in Sophos Endpoint Security and Control gescannt.

7.10.2.2 Aktivieren der Kontrolle unangebrachter Websites

Zum Aktivieren von Web Control in Enterprise Console und zur Verwendung der Kontrolle unangebrachter Websites verfahren Sie wie folgt:

Hinweis: Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Web Control** verfügen, um eine Web Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 17) entnehmen.

So aktivieren Sie die Kontrolle unangebrachter Websites:

1. Prüfen Sie, welche Web Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten. Weitere Informationen finden Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Web Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Web Control-Richtlinie** wird angezeigt.

3. Wählen Sie auf der Registerkarte **Allgemein** die Option **Web Control aktivieren**.

   Die Richtlinie zur **Kontrolle unangebrachter Websites** wird angezeigt. Sie können die den 14 Kategorien zugewiesenen Standardmaßnahmen nach Belieben anpassen. Weitere Informationen finden Sie unter *Auswahl einer Maßnahme zu Website-Kategorien* (Seite 197).

7.10.2.3 Website-Kategorien

Die Funktion zur **Kontrolle unangebrachter Websites** umfasst 14 Kategorien zur Kontrolle der Inhalte, die Benutzer im Browser aufrufen können. Weitere Informationen finden Sie unter *Informationen zur Kontrolle unangebrachter Websites* (Seite 193).

Die im Folgenden beschriebenen Website-Kategorien werden gefiltert. Die Standardmaßnahme für die jeweilige Kategorie wird in Klammern angegeben. Kategorien können jeweils als **Blockieren**, **Warnen** oder **Zulassen** eingestuft werden. Wenn die Option **Zulassen** ausgewählt

wird, kann der Benutzer auf alle Seiten in der Kategorie zugreifen. Anweisungen zum Ändern der Maßnahme finden Sie unter *Auswahl einer Maßnahme zu Website-Kategorien* (Seite 197).

- **Pornografie (Blockieren)**: Die Kategorie umfasst unter anderem pornografische Produkte wie Sexspielzeug, CD-ROMs, Videos, Kinderpornografie (einschließlich der IWF-Liste), Dienstleistungen für Erwachsene, wie Videokonferenzen, Begleitdienste, Strip-Clubs; Geschichten mit erotischen Inhalten und Schilderungen sexueller Handlungen; pornografische Cartoons und Animationen; Online-Gruppen oder Foren mit sexuellen Inhalten; Seiten mit sexueller oder erotischer Ausrichtung mit vollständiger oder teilweiser Nacktheit; Abbildungen sexueller Handlungen Text oder Grafiken in Zusammenhang mit sexueller Ausbeutung oder Gewalt. Sonstige Darstellungen von Nacktheit.

  Hinweis: Seiten (ohne grafische Beispiele) zu Sexualkrankheiten und Brustkrebs sind nicht enthalten

- **Genussmittel (Warnen)**: Die Kategorie umfasst Seiten zum Vertrieb von oder der Werbung für Alkohol und Tabak (kostenlos oder gebührenpflichtig).
- **Anonymisierende Proxys (Blockieren)**: Die Kategorie umfasst Seiten für Remote-Proxyserver oder anonymes Browsen, Suchmaschinen-Cache-Speicher, die Filter umgehen und Web-Translator, die Filter umgehen.
- **Kriminelle Handlungen (Blockieren)**: Die Kategorie umfasst Seiten, die kriminelle Handlungen verherrlichen oder Anweisungen zum Durchführen krimineller Handlungen bieten.
- **Glücksspiel (Warnen)**: Die Kategorie umfasst Online-Glücksspiel- oder Lotterie-Seiten, auf denen echtes oder virtuelles Geld ausgegeben wird; Seiten mit Informationen zum Abgeben von Wetten, zur Teilnahme an Lotterien, Glücksspiel oder Zahlenziehungen; virtuelle Casinos und Offshore-Glücksspiel; Sportwetten; virtuelle Sportligen, die hohe Gewinne versprechen oder einen hohen Wetteinsatz verlangen.
- **Hacking (Blockieren)**: Die Kategorie umfasst Seiten, die die fragwürdige oder illegale Verwendung von Ausrüstung und Software zum Hacken von Kennwörtern, der Erstellung von Viren oder dem Zugriff auf Computer oder computerbasierte Kommunikationssysteme anpreist oder erläutert; Seiten mit Anweisungen oder Workarounds zum Filtern von Software; Cracks; Warez, illegale Download-Seiten und Seiten in Zusammenhang mit Computerkriminalität.
- **Harte Drogen (Blockieren)**: Die Kategorie umfasst Seiten mit Rezepten, Anweisungen bzw. Kits zur Herstellung oder dem Anbau illegaler Stoffe; der Verherrlichung, Empfehlung oder Anweisung zur Verschleierung des Konsums von Alkohol, Tabak, illegalen Drogen oder anderen Substanzen, die nicht von Minderjährigen konsumiert werden dürfen; Informationen zu "legalen Highs", wie etwa Klebstoffschnüffeln, Medikamentenmissbrauch oder dem Missbrauch anderer legalen Substanzen; der (kostenlosen oder gebührenpflichtigen) Verbreitung illegaler Drogen; der Darstellung, dem Vertrieb oder der Beschreibung von Drogenzubehör.
- **Intolerantes Verhalten (Blockieren)** : Die Kategorie umfasst Seiten, die die Degradierung von oder Angriffe auf bestimmte Bevölkerungsschichten oder Institutionen aufgrund von Religion, Rasse, Nationalität, Geschlecht, Alter, Behinderung oder sexueller Ausrichtung fördern oder dazu auffordern; Seiten, die eine politische oder gesellschaftliche Auffassung vertreten, deren Anhänger sich selbst als überlegen ansehen oder die bestimmte Gruppen

aufgrund von Rasse, Religion, Nationalität, Geschlecht, Alter, Behinderung oder sexueller Ausrichtung ausschließen; Seiten, auf denen der Holocaust verleugnet oder unsachgemäß dargestellt wird sowie sonstige geschichtsverzerrende Seiten; Seiten, die die Mitgliedschaft in Gangs[1] oder Kultvereinigungen[2] erzwingen wollen oder Mitglieder für solche Vereinigungen anwerben; militante oder extremistische Seiten; Seiten mit außerordentlich unsensiblen oder anstößigen Inhalten, einschließlich von Seiten, die sich despektierlich über andere Glaubensrichtungen oder Weltanschauungen äußern oder diese nicht anerkennen.

Hinweis: Nachrichten, historische Berichte oder Presseberichte, die unter Umständen die genannten Kriterien erfüllen (grafische Beispiele ausgenommen), werden nicht blockiert.

[1]Gangs sind Gruppen, deren Hauptaktivität in der Organisation krimineller Handlungen besteht. Sie verfügen über einen Namen oder ein Erkennungszeichen, und die Mitglieder begehen individuell oder im Kollektiv Straftaten im Namen der Gruppe.

[2] Unter Kultvereinigungen sind Gruppen zu verstehen, deren Mitglieder auf manipulative Weise angeworben und durch ungebührliche Einflussnahme (Persönlichkeits- und Verhaltensveränderungen) gebunden wurden; die Führungsspitze der Gruppen ist allmächtig, ihre Ideologie totalitär und Individuen werden der Gruppe untergeordnet; die Gruppe positioniert sich außerhalb der Gesellschaft.

- **Phishing und Betrug (Blockieren)**: Die Kategorie umfasst Seiten in Zusammenhang mit Phishing und Telefonbetrug, Seiten mit Tipps zum Diebstahl von Dienstleistungen, Plagiat und Betrug sowie Seiten, auf denen akademische Arbeiten feilgeboten werden.
- **Spam-URLs (Blockieren)**: Die Kategorie umfasst URLs, die in Spam vorkommen. Sie fallen unter anderem in folgende Themenbereiche: Computer, Finanzen und Aktien, Unterhaltung, Spiele, Gesundheit und Arzneimittel, Humor und Kurioses, Dating, Produkte und Dienstleistungen, Shopping, Reisen.
- **Spyware (Blockieren)**: Die Kategorie umfasst Seiten, die die Erfassung oder Verfolgung von Daten anbieten oder anpreisen (ohne Kenntnis oder ausdrückliche Zustimmung des Endbenutzers oder Unternehmens). Hierzu zählen schädliche ausführbare Dateien oder Viren, Überwachungssoftware sowie unerwünschte gewerbliche Software, Spyware und Call Home-Malware.
- **Geschmackloser, anstößiger Inhalt (Warnen)**: Die Kategorie umfasst Seiten mit anstößiger oder gewaltverherrlichender Sprache (Witze, Comics, Satire) und unverhältnismäßig vielen Schimpfwörtern oder obszönen Gesten.
- **Gewalt (Warnen)**: Die Kategorie umfasst Seiten, die gewalttätige Übergriffe auf Menschen, Tiere oder Einrichtungen darstellen, beschreiben oder ermutigen; Abbildungen von Folter, Verstümmlung, Blut oder schrecklichen Todesszenen; Förderung, Ermutigung oder Darstellung von Selbstverletzung oder Selbstmord (auch durch Essstörungen oder Sucht); Anweisungen oder Kits zum Erstellen von Bomben oder anderen zerstörerischen Gegenständen; Seiten, die Terrorismus verherrlichen; Gewaltsport oder gewaltverherrlichende Spiele (inkl. Video- und Online-Spiele).

  Hinweis: Nachrichten, historische Berichte oder Presseberichte, die unter Umständen die genannten Kriterien erfüllen (grafische Beispiele ausgenommen), werden nicht gesperrt.

- **Waffen (Warnen)**: Die Kategorie umfasst Seiten zum Online-Verkauf oder Seiten mit Bestellinformationen wie Preislisten oder Händlerstandorten; Seiten, die vornehmlich

Inhalte in Zusammenhang mit dem Verkauf von Schießwaffen, Waffen, Munition oder Giftstoffen aufweisen oder auf solche Seiten verlinken; Klubs, die Waffentraining mit Maschinengewehren, Automatikwaffen oder sonstigen Angriffswaffen sowie Sniper-Training anbieten.

Hinweis: Waffen werden als Gegenstände (beispielsweise Schläger, Messer oder Gewehr) definiert, die zur Verletzung, zum Besiegen oder Zerstören eingesetzt werden.

7.10.2.4 Auswahl einer Maßnahme zu Website-Kategorien

Wenn Web Control aktiviert ist und Sie die Richtlinie zur **Kontrolle potenziell unangebrachter Websites** aktiviert haben, können Sie den jeweiligen Kategorien Maßnahmen zuordnen. Zudem können Sie auf der Basis der Standardrichtlinie eine neue Richtlinie erstellen. Weitere Informationen finden Sie unter *Erstellen einer Richtlinie* (Seite 35).

So wählen Sie eine Maßnahme zu Website-Kategorien aus:

1. Wählen Sie in der Registerkarte **Allgemein**, im Dropdown-Menü neben der gewünschten Kategorie eine der folgenden Maßnahmen aus:
   - **Blockieren**: Der Benutzer kann Seiten in dieser Kategorie nicht aufrufen. Bei HTTP-Seiten wird der Benutzer darüber informiert, dass die Seite blockiert wurde und warum. Bei HTTPs-Seiten erscheint eine Sprechblasenmeldung in der Symbolleiste von Windows.
   - **Warnen**: Der Benutzer wird gewarnt, dass er den Internetnutzungsrichtlinien des Unternehmens zuwider handelt. Der Vorgang kann jedoch fortgesetzt werden. Bei HTTP-Seiten wird ein Warnhinweis zum Aufrufen der Seite angezeigt. Bei HTTPS-Seiten werden Benutzer nicht benachrichtigt und die Seite kann aufgerufen werden. In Enterprise Console wird ein „Fortsetzen"-Ereignis protokolliert.
   - **Zulassen**: Benutzer können Seiten in der Kategorie aufrufen. Es wird kein Ereignis protokolliert.
2. Klicken Sie auf **OK**.

7.10.2.5 Verwalten von Website-Ausschlüssen

Wenn Sie die Richtlinie zur **Kontrolle potenziell unerwünschter Websites** ausgewählt haben, können Sie Ausschlüsse zu den Maßnahmen „Blockieren" und „Warnen" festlegen. Sie können Websites ausschließen, indem Sie sie in die Liste zulässiger oder blockierter Websites aufnehmen. Einträge können in Form von IP-Adressen oder Domänennamen vorliegen. Zudem können Sie vorhandene Website-Einträge bearbeiten bzw. von einer Liste entfernen.

Hinweis: Bei Überschneidungen bzw. Konflikten zwischen den Maßnahmen „Blockieren" und „Zulassen" hat die Maßnahme „Blockieren" Vorrang. Wenn die gleiche IP-Adresse etwa in der Liste „Blockieren" und „Zulassen" enthalten ist, wird die Website blockiert. Wenn ferner eine Domäne in der Liste Blockieren", eine ihrer Unterdomänen jedoch in der Liste „Zulassen" enthalten ist, werden die Domäne und sämtliche Unterdomänen blockiert.

So fügen Sie Website-Ausschlüsse hinzu:

1. Klicken Sie auf der Registerkarte **Website-Ausschlüsse** auf die Schaltfläche **Hinzufügen** neben dem Textfeld **Zugelassene Websites** oder **Gesperrte Websites**.

2. Klicken Sie im Dialogfeld **Zulässige Website hinzufügen** auf **Domänenname**, **IP-Adresse mit Subnetz-Maske** oder **IP-Adresse**. Über den Textfeldern finden Sie jeweils Beispiele für das Format.
3. Geben Sie iin das Textfeld den Domänennamen oder die IP-Adresse der Website ein, die Sie zulassen oder blockieren möchten.
4. Klicken Sie auf **OK**.

Wenn Sie Websites bearbeiten oder aus eine Liste entfernen möchten, wählen Sie die Website aus und klicken Sie auf **Bearbeiten** oder **Entfernen**.

7.10.3 Vollständige Web Control

7.10.3.1 Vollständige Web Control

Hinweis: Die Funktion ist nicht im Umfang aller Lizenzen enthalten. Wenn Sie die Funktion nutzen möchten, müssen Sie eine entsprechende Lizenz erwerben. Nähere Informationen finden Sie unter *http://www.sophos.com/de-de/products/complete/comparison.aspx*.

Wenn Sie eine Sophos Web Appliance oder eine Security Management Appliance im Einsatz haben, können Sie mit Enterprise Console Appliance-basierte Richtlinien an die Benutzer verteilen.

Die Endpoints der Benutzer kommunizieren mit Enterprise Console genau wie bei Auswahl der Richtlinie zur Kontrolle unangebrachter Websites. Die Web-Filter-Regeln und Protokolle zur Web-Aktivität werden mit der angegebenen Sophos Web Appliance oder Management Appliance synchronisiert. Die Richtlinie wird auf der Basis der aktuellen Sophos Daten auf dem Endpoints des Benutzers gespeichert und darauf übertragen.

In Einklang mit der Web Control-Richtlinie werden angeforderte Websites blockiert oder zugelassen oder es wird eine Warnung an den Benutzer ausgegeben. Die Funktionen **Reports** und **Suche** der Web Appliance bzw. der Management Appliance gibt Aufschluss über die Aktivitätsdaten der Benutzer. Die Ereignisse „Blockieren“, „Warnen“und „Zulassen“ werden auf der Appliance festgehalten. Seiten, die von der Live-URL-Filterfunktion von Sophos Endpoint Security and Control (Web-Schutz) analysiert und gescannt werden, werden in Enterprise Console als Web-Ereignisse verzeichnet.

Hinweis: Sowohl HTTP- als auch HTTPS-Websites werden zwar in allen unterstützten Browsern gefiltert, die Benutzerbenachrichtigungen unterscheiden sich jedoch. Bei HTTP-Seiten werden Benutzer über Seiten benachrichtigt, die in die Kategorie „Blockieren“ oder „Warnen“ fallen. Bei HTTPS werden Benutzer lediglich über Seiten aus der Kategorie „Blockieren“ in Form einer Sprechblasenmeldung in der Symbolleiste von Windows informiert. „Warn“-Maßnahmen werden bei HTTPS weder angezeigt noch blockiert. Benutzer können die gewünschte Seite aufrufen. Das Ereignis wird in der Web Appliance oder der Management Appliance als Ereignis „Fortsetzen“ protokolliert.

Sie können die Web Appliance oder die Management Appliance jedoch auch zur Verwendung von LiveConnect konfigurieren. So werden Richtlinien-Updates auf die Benutzer übertragen. Report-Daten von den Endpoints werden auch dann hochgeladen, wenn keine Verbindung zum Netzwerk besteht.

Bei Auswahl der Option **Vollständige Web Control** wird eine umfassende Richtlinie umgesetzt. Die vollständige Web Control bietet folgende Vorteile gegenüber der Basisversion:

- Websites werden in 50 Kategorien unterteilt. Dementsprechend werden Warnmeldungen an die Benutzer ausgegeben oder Anfragen werden blockiert.
- Es können Richtlinien für bestimmte Zeiträume festgelegt werden.
- Zahlreiche Richtlinien können als Benutzer- oder Gruppenausschlüsse der Standard- und zeitlich gebundenen Zugriffsrichtlinie eingesetzt werden.
- Auf der Web Appliance oder der Management Appliance stehen ausführliche Protokolle und Reports zur Verfügung.
- Mit LiveConnect können Richtlinien-Updates verteilt und Report-Daten hochgeladen werden, selbst wenn Benutzer remote arbeiten.
- Benutzer können Anregungen zum Umgang mit blockierten URLs machen.
- Benutzerdefinierte Benachrichtigungen mit dem Logo Ihres Unternehmens sowie entsprechender Text können angezeigt werden. Nähere Informationen entnehmen Sie bitte der Dokumentation zur Sophos Web Appliance (in englischer Sprache).
- Bei Aktivierung von „SafeSearch“ wird das Aufrufen fragwürdiger Websites aus Suchmaschinen automatisch aktiviert.

Weitere Informationen zum Einrichten einer vollständigen Web Appliance-Richtlinie finden Sie in der Dokumentation zu Sophos Web Appliance unter *http://wsa.sophos.com/docs/wsa/*.

7.10.3.2 Aktivieren der Vollständigen Web Control

Hinweis: Im Folgenden wird davon ausgegangen, dass Sie über eine konfigurierte, voll funktionsfähige Sophos Web Appliance oder Management Appliance verfügen und Endpoint Web Control nutzen.

Die Web Control-Richtlinie ist standardmäßig deaktiviert. Führen Sie die folgenden Schritte durch, um Web Control zu aktivieren und die Richtlinie der Vollständigen Web Control zu verwenden.

Hinweis: Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Web Control** verfügen, um eine Web Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 17) entnehmen.

So aktivieren Sie die Vollständige Web Control:

1. Prüfen Sie, welche Web Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten. Weitere Informationen finden Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Web Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Web Control-Richtlinie** wird angezeigt.

3. Klicken Sie auf der Registerkarte **Allgemein** die Option **Web Control aktivieren**.
4. Wählen Sie die Option **Vollständige Web Control**.
5. Geben Sie in das Feld **Einstellungen** den **Appliance-Hostnamen** ein: Sie müssen einen voll qualifizierten Hostnamen angeben.
6. Geben Sie im Feld **Einstellungen** den **Sicherheitsschlüssel für Richtlinienaustausch** an. Der Schlüssel muss mit dem auf der Seite **Endpoint Web Control** der Sophos Appliance angezeigten Schlüssel übereinstimmen. Nähere Informationen entnehmen Sie bitte der Dokumentation zur Sophos Web Appliance unter *http://wsa.sophos.com/docs/wsa/*.
7. Auf Wunsch können Sie auch die die Option **Browsen verweigern, wenn die Website-Kategorie nicht bestimmt werden kann** auswählen. Wenn ein Endpoint keine Daten zu den Website-Kategorien abrufen kann, werden nicht kategorisierbare URLs solange blockiert, bis der Dienst wieder funktioniert.

   Die Option ist standardmäßig nicht aktiviert. Benutzer können also browsen, wenn die Kategorisierung nicht funktioniert.

8. Klicken Sie auf **OK**.

   Enterprise Console konfiguriert die Endpoints zur Kommuniaktion mit der Web Appliance oder der Management Appliance.

8 Einrichten von Alerts und Benachrichtigungen

8.1 Was sind Alerts und Benachrichtigungen?

In Enterprise Console werden mehrere Benachrichtigungsmethoden verwendet.

- **In der Konsole angezeigte Alerts**

  Wenn ein Objekt auf einem Computer gefunden wird, das bearbeitet werden muss, oder ein Fehler aufgetreten ist, sendet Sophos Endpoint Security and Control einen Alert an Enterprise Console. Der Alert wird in der Computerliste angezeigt. Nähere Informationen zum Umgang mit solchen Alerts können Sie dem Abschnitt *Umgang mit Alerts zu erkannten Objekten* (Seite 60) entnehmen.

  Diese Alerts werden immer angezeigt. Sie müssen nicht eingerichtet werden.

- **In der Konsole angezeigte Ereignisse**

  Application Control-, Firewall-, Patchanalyse-, Web Control-, Data Control-, Device Control-, Verschlüsselungs- oder Manipulationsschutz-Ereignisse auf einem Endpoint (z.B. die Firewall hat eine Anwendung blockiert) werden an Enterprise Console übertragen und können in der jeweiligen Ereignisanzeige abgerufen werden.

- **Von der Konsole an die ausgewählten Empfänger gesendete Alerts und Benachrichtigungen**

  Wenn ein Objekt auf einem Computer gefunden wird, erscheint auf dem Computer-Desktop standardmäßig eine Meldung und zum Windows Ereignisprotokoll wird ein Eintrag hinzugefügt. Bei Application Control-, Data Control- oder Device Control-Ereignissen erscheint eine Nachricht auf dem Desktop.

  Sie können außerdem E-Mail-Benachrichtigungen oder SNMP-Benachrichtigungen für Administratoren einrichten.

  Hinweis: Anweisung zur Verwendung authentifizierter SMTP-Benachrichtigungen entnehmen Sie bitte dem Support-Artikel 113780 (*http://www.sophos.de/support/knowledgebase/article/113780.html*).

In diesem Abschnitt wird die Einrichtung von Benachrichtigungen erläutert, die an die von Ihnen gewählten Empfänger gesendet werden.

8.2 Einrichten von Softwareabonnement-Alerts

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Systemkonfiguration** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Update Manager-Alerts werden in Enterprise Console in der Spalte **Alerts** in der Ansicht **Update Manager** angezeigt. Wenn Sie eine bestimmte Softwareversion abonniert haben, wird ein Alert angezeigt, wenn die Version demnächst eingestellt wird oder eingestellt wurde. Auch bei Änderungen der Produktlizenz wird ein Alert angezeigt.

Wenn Sie die Option **Nicht mehr unterstützte Software einer bestimmten Version automatisch updaten** gewählt haben, wird das Abonnement automatisch aktualisiert.

Wenn Sie sich nicht für automatische Upgrades entschieden haben, werden Sie zur Änderung Ihres Abonnements aufgefordert.

Wichtig: Wenn Sie nicht unterstützte Software nutzen, sind Ihre Computer vor neuen Threats nicht sicher. Es wird daher empfohlend, umgehend auf eine unterstützte Version zu aktualisieren.

Sie können Ihre gewählten Empfänger per E-Mail über (baldige) Produkteinstellungen benachrichtigen lassen.

1. Wählen Sie im Menü **Extras** die Option **E-Mail-Benachrichtigungen konfigurieren**.

   Das Dialogfeld **E-Mail-Benachrichtigungen konfigurieren** wird angezeigt.

2. Wenn die SMTP-Einstellungen nicht konfiguriert wurden oder wenn Sie die Einstellungen ansehen oder ändern möchten, klicken Sie auf **Konfigurieren**.

   Geben Sie in das Dialogfeld **SMTP-Einstellungen konfigurieren** Folgendes ein:

   a) Geben Sie in das Textfeld **Serveradresse** den Hostnamen oder die IP-Adresse des SMTP-Servers ein.

   b) Geben Sie in das Textfeld **Absender** eine E-Mail-Adresse ein, an die nicht zustellbare Benachrichtigungen und Nicht-Zustellbarkeitsmeldungen gesendet werden können.

   c) Klicken Sie auf **Test**, um die Verbindung zu testen.

3. Klicken Sie im Bereich **Empfänger** auf **Hinzufügen**.

   Das Dialogfeld **Neuer E-Mail-Benachrichtigungsempfänger** wird angezeigt.

4. Geben Sie in das Feld **E-Mail-Adresse** die Adresse des Empfängers ein.
5. Wählen Sie im Feld **Sprache** die Sprache, in der E-Mail-Benachrichtigungen gesendet werden sollen.
6. Wählen Sie im Fensterbereich **Abonnements** unter „Software-Abonnenments“ die E-Mail-Benachrichtigungen unter „Update Manager“, die Sie an diesen Empfänger senden möchten. Sie können sich über folgende Ereignisse benachrichtigen lassen:

   - Eine von Ihnen abonnierte Produktversion wird demnächst von Sophos eingestellt.
   - Eine von Ihnen abonnierte Produktversion ist nicht mehr verfügbar.

     Wenn ein abonniertes Produkt eingestellt wurde oder Sie Ihre Lizenz geändert haben und die neue Lizenz das Produkt nicht mehr enthält, wird die Benachrichtigung versendet.

   - Die Sophos Lizenzdaten wurden aktualisiert. Unter Umständen haben sich Produktfunktionen geändert.

8.3 Einrichten von Antivirus- und HIPS-E-Mail-Benachrichtigungen

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Wenn auf einem Computer in einer Gruppe ein Virus, verdächtiges Verhalten oder eine unerwünschte Anwendung erkannt wurde oder ein Fehler aufgetreten ist, kann an diesen Computer eine entsprechende E-Mail-Benachrichtigung gesendet werden.

Wichtig: Mac OS X Computer können E-Mail-Benachrichtigungen nur an eine Adresse senden.

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf die Antivirus- und HIPS-Richtlinie, die Sie ändern möchten.
2. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** auf **Benachrichtigungen**.
3. Öffnen Sie im Dialogfeld **Benachrichtigungen** die Registerkarte **E-Mail-Benachrichtigungen** und wählen Sie **E-Mail-Benachrichtigungen aktivieren**.
4. Wählen Sie unter **Bei folgenden Ereignissen eine Benachrichtigung senden:** die Ereignisse aus, zu denen jeweils eine E-Mail-Benachrichtigung gesendet werden soll.

   Hinweis: Die Einstellungen zur **Erkennung verdächtigen Verhaltens**, **Erkennung verdächtiger Dateien** und zur **Erkennung und Bereinigung von Adware und PUA** gelten nur für Windows 2000 und aufwärts. Die Einstellung für **Sonstige Fehler** trifft nur für Windows zu.

5. Sie können im Bereich **Empfänger** durch Klicken auf **Hinzufügen** oder **Entfernen** die E-Mail-Adressen bestimmen, an die Benachrichtigungen gesendet werden sollen. Klicken Sie auf **Umbenennen**, um die E-Mail-Adresse zu ändern, die Sie hinzugefügt haben.

   Wichtig: Mac OS X-Computer senden Benachrichtigungen nur an den ersten Empfänger in der Liste.

6. Klicken Sie auf die Schaltfläche **SMTP konfigurieren**, um die Einstellungen für den SMTP-Server und die Sprache der E-Mail-Benachrichtigungen zu ändern.

7. Geben Sie in das Dialogfeld **SMTP-Einstellungen konfigurieren** Folgendes ein:
   - Geben Sie in das Textfeld **SMTP-Server** den Hostnamen oder die IP-Adresse des SMTP-Servers ein. Klicken Sie auf **Test**, um eine Test-E-Mail-Benachrichtigung zu senden.
   - Geben Sie in das Textfeld **SMTP-Absenderadresse** eine E-Mail-Adresse ein, an die nicht zustellbare Benachrichtigungen und Nicht-Zustellbarkeitsmeldungen gesendet werden sollen.
   - Im Textfeld **SMTP-Adresse für Rückantworten:** können Sie eine E-Mail-Adresse angeben, an die Antworten auf E-Mail-Benachrichtigungen gesendet werden können. E-Mail-Benachrichtigungen werden von einem Systemkonto gesendet.
   - Klicken Sie im Bereich **Sprache** auf den Drop-Down-Pfeil und wählen Sie die Sprache, in der die E-Mail-Benachrichtigungen gesendet werden sollen.

8.4 Einrichten von Antivirus- und HIPS-SNMP-Benachrichtigungen

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können SNMP-Benachrichtigungen an bestimmte Benutzer senden, wenn auf einem der Computer in der Gruppe ein Virus erkannt wurde oder ein Fehler aufgetreten ist.

Hinweis: Diese Einstellungen gelten nur für Systeme unter Windows 2000 und aufwärts.

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf die Antivirus- und HIPS-Richtlinie, die Sie ändern möchten.
2. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** auf **Benachrichtigungen**.
3. Öffnen Sie im Dialogfeld **Benachrichtigungen** die Registerkarte **SNMP-Benachrichtigungen** und wählen Sie **SNMP-Benachrichtigungen aktivieren**.
4. Wählen Sie im Bereich **Bei folgenden Ereignissen eine Benachrichtigung senden:** die Ereignisse aus, bei deren Eintritt SNMP-Benachrichtigungen gesendet werden sollen.
5. Geben Sie im Textfeld **SNMP-Trapziel:** die IP-Adresse des Empfängers an.
6. Geben Sie im Textfeld **SNMP-Community:** den Namen der SNMP-Community an.

8.5 Konfigurieren von Antivirus- und HIPS-Desktop-Benachrichtigungen

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.

- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Standardmäßig werden Benachrichtigungen auf dem Computer angezeigt, auf dem ein Virus, verdächtiges Objekt oder eine potenziell unerwünschte Anwendung gefunden wurde. Diese Benachrichtigungen lassen sich konfigurieren.

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf die Antivirus- und HIPS-Richtlinie, die Sie ändern möchten.
2. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** auf **Benachrichtigungen**.
3. Klicken Sie im Dialogfeld **Benachrichtigungen** auf die Registerkarte **Desktop-Benachrichtigungen**.

   Standardmäßig ist **Desktop-Benachrichtigungen aktivieren** mitsamt allen Optionen im Bereich **Bei folgenden Ereignissen eine Benachrichtigung senden** ausgewählt. Ändern Sie diese Einstellungen gegebenenfalls.

   Hinweis: Die Einstellungen zur **Erkennung verdächtigen Verhaltens**, **Erkennung verdächtiger Dateien** und zur **Erkennung von Adware und PUA** gelten nur für Windows 2000 und aufwärts.

4. Sie können im Textfeld **Benutzerdefinierter Text** eine Benachrichtigung eingeben, die an das Ende der Standard-Desktop-Benachrichtigung angehängt wird.

8.6 Einrichten von Application Control-Alerts und -Benachrichtigungen

Bei rollenbasierter Verwaltung:

- Zur Konfiguration einer Application Control-Richtlinie müssen Sie über die Berechtigung **Richtlinieneinstellungen – Application Control** verfügen.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Ausgewählte Benutzer können benachrichtigt werden, wenn auf einem Computer eine Controlled Application erkannt wird.

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf die gewünschte Application Control-Richtlinie.
2. Öffnen Sie im Dialogfeld **Application Control-Richtlinie** die Registerkarte **Benachrichtigung**.

   Im Bereich **Benachrichtigung** ist das Kontrollkästchen **Desktop-Benachrichtigung aktivieren** standardmäßig aktiviert. Wenn eine nicht zugelassene Controlled Application von On-Access-Scans erkannt und blockiert wird, wird eine Desktop-Benachrichtigung angezeigt, die den Benutzer darüber informiert, dass die Anwendung gesperrt wurde.

3. Sie können im Feld **Text** eine Meldung eingeben, die an eine Desktop-Benachrichtigung angehängt wird.

4. Aktivieren Sie die Option **E-Mail-Benachrichtigung aktivieren**, wenn zu erkannten Controlled Applications eine E-Mail-Benachrichtigung gesendet werden soll.
5. Wenn SNMP-Benachrichtigungen gesendet werden sollen, wählen Sie die Option **SNMP-Benachrichtigungen aktivieren**.

   Hinweis: Ihre Antivirus- und HIPS-Richtlinieneinstellungen legen die Konfiguration und die Empfänger von E-Mail- und SNMP-Benachrichtigungen fest. Weitere Informationen finden Sie unter *Einrichten von Antivirus- und HIPS-SNMP-Benachrichtigungen* (Seite 204).

8.7 Einrichten von Data Control-Alerts und -Benachrichtigungen

Bei rollenbasierter Verwaltung:

- Zum Konfigurieren einer Device Control-Richtlinie ist die Berechtigung **Richtlinieneinstellung – Data Control** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Enterprise Console meldet die Erkennung bzw. Blockierung sensibler Daten mit Hilfe von Ereignissen und Benachrichtigungen.

Nähere Informationen zu Data Control-Richtlinien und -Ereignissen finden Sie im Abschnitt *Data Control* (Seite 156).

Wenn Data Control aktiv ist, werden die folgenden Ereignisse und Benachrichtigungen standardmäßig protokolliert oder angezeigt:

- Data Control-Ereignisse werden auf dem Arbeitsplatzrechner protokolliert.
- Data Control-Ereignisse werden an Enterprise Console gesendet und können in der **Data Control – Ereignisanzeige** angezeigt werden. (Klicken Sie im Menü **Ereignisse** auf **Data Control-Ereignisse**.)

  Hinweis: Endpoints können bis zu 50 Data Control-Ereignisse pro Stunde an Enterprise Console senden.

- Auf dem Dashboard wird die Anzahl der Computer angezeigt, auf denen die Summe der Data Control-Ereignisse in den vergangenen 7 Tagen den angegebenen Höchstwert überschritten hat.
- Desktop-Benachrichtigungen werden auf dem Arbeitsplatzrechner angezeigt.

In Enterprise Console lassen sich folgende Benachrichtigungen einrichten:

E-Mail-Benachrichtigungen	E-Mail-Benachrichtigungen werden an die von Ihnen gewählten Empfänger gesendet.
SNMP-Benachrichtigungen	SNMP-Benachrichtigungen werden an die von Ihnen in den Einstellungen der Anti-Virus- und HIPS-Richtlinie festgelegten Empfänger gesendet.

So richten Sie Data Control-Benachrichtigungen ein:

1. Prüfen Sie, welche Data Control-Richtlinie von der/den Computergruppe/n verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).

2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Data Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

   Das Dialogfeld **Data Control-Richtlinie** wird angezeigt.

3. Öffnen Sie im Dialogfeld **Data Control-Richtlinie** die Registerkarte **Benachrichtigungen**. Desktop-Benachrichtigungen und die Option **Passende Regeln in Benachrichtigungen einbeziehen** sind standardmäßig aktiviert.
4. Sie können Ihre eigenen Meldungen zu den Standardmeldungen hinzufügen. Diese werden angezeigt, wenn der Benutzer zur Bestätigung von Dateiübertragung oder von blockiertem Datenverkehr aufgefordert wird.

   Sie können maximal 100 Zeichen eingeben. Sie können auch einen HTML-Link in die Nachricht aufnehmen, z.B. Über Sophos.

5. Wenn Sie E-Mail-Benachrichtigungen wünschen, aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen aktivieren**. Geben Sie in das Feld **E-Mail-Empfänger** die E-Mail-Adressen der gewünschten Empfänger ein. Trennen Sie die Adressen durch ein Semikolon (;) voneinander ab.
6. Wenn Sie SNMP-Benachrichtigungen aktivieren möchten, markieren Sie das Kontrollkästchen **SNMP-Benachrichtigungen aktivieren**.

   Die Einstellungen für E-Mail-Server und SNMP-Traps werden über die Anti-Virus- und HIPS-Richtlinie vorgenommen.

8.8 Einrichten von Device Control-Alerts und -Benachrichtigungen

Bei rollenbasierter Verwaltung:

- Sie müssen über die Berechtigung **Richtlinieneinstellung – Device Control** verfügen, um eine Device Control-Richtlinie bearbeiten zu können.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Enterprise Console meldet die Erkennung bzw. Blockierung gesteuerter Geräte mit Hilfe von Ereignissen und Benachrichtigungen.

Nähere Informationen zu Device Control-Richtlinien und -ereignissen finden Sie im Abschnitt *Device Control* (Seite 171).

Wenn Device Control aktiv ist, werden die folgenden Ereignisse und Benachrichtigungen standardmäßig protokolliert oder angezeigt:

- Device Control-Ereignisse werden auf dem Arbeitsplatzrechner protokolliert.

- Device Control-Ereignisse werden an Enterprise Console gesendet und können in der **Device Control – Ereignisanzeige** angezeigt werden. (Klicken Sie im Menü **Ereignisse** auf **Device Control-Ereignisse**.)
- Auf dem Dashboard wird die Anzahl der Computer angezeigt, auf denen die Summe der Device Control-Ereignisse in den vergangenen 7 Tagen den angegebenen Höchstwert überschritten hat.
- Desktop-Benachrichtigungen werden auf dem Arbeitsplatzrechner angezeigt.

In Enterprise Console lassen sich folgende Benachrichtigungen einrichten:

E-Mail-Benachrichtigungen	E-Mail-Benachrichtigungen werden an die von Ihnen gewählten Empfänger gesendet.
SNMP-Benachrichtigungen	SNMP-Benachrichtigungen werden an die von Ihnen in den Einstellungen der Anti-Virus- und HIPS-Richtlinie festgelegten Empfänger gesendet.

So können Sie Device Control-Benachrichtigungen einrichten:

1. Prüfen Sie, welche Device Control-Richtlinie von den Computergruppen verwendet wird, die Sie konfigurieren möchten.

   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Device Control**. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.
3. Desktop-Benachrichtigungen sind im Dialogfeld **Device Control-Richtlinie** auf der Registerkarte **Benachrichtigungen** standardmäßig aktiviert. Wenn Sie weitere Änderungen an der Konfiguration von Benachrichtigungen vornehmen möchten, verfahren Sie wie folgt:

   - *Verfassen eines Texts für Desktop-Benachrichtigungen*: Geben Sie in das Feld **Text** den gewünschten Text ein. Der Text wird an das Ende einer Standard-Benachrichtigung angehängt.

     Sie können maximal 100 Zeichen eingeben. Sie können auch einen HTML-Link in die Nachricht aufnehmen, z.B. Über Sophos.
   - *Aktivieren von E-Mail-Benachrichtigungen*: Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen aktivieren**. Geben Sie in das Feld **E-Mail-Empfänger** die E-Mail-Adressen der gewünschten Empfänger ein. Trennen Sie die Adressen durch ein Semikolon (;) voneinander ab.
   - *Aktivieren von SNMP-Benachrichtigungen*: Aktivieren Sie das Kontrollkästchen **SNMP-Benachrichtigungen aktivieren**.

   Die Einstellungen für E-Mail-Server und SNMP-Traps werden über die Anti-Virus- und HIPS-Richtlinie vorgenommen.

8.9 Einrichten von Netzwerkstatus-E-Mail-Benachrichtigungen

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren der Netzwerkstatus-E-Mail-Benachrichtigungen über die Berechtigung **Systemkonfiguration** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können E-Mail-Benachrichtigungen einrichten, die an die gewählten Empfänger gesendet werden sollen, wenn eine Warnstufe oder eine kritische Stufe für einen Dashboard-Bereich überschritten wird.

1. Wählen Sie im Menü **Extras** die Option **E-Mail-Benachrichtigungen konfigurieren**.

   Das Dialogfeld **E-Mail-Benachrichtigungen konfigurieren** wird angezeigt.

2. Wenn die SMTP-Einstellungen nicht konfiguriert wurden oder wenn Sie die Einstellungen ansehen oder ändern möchten, klicken Sie auf **Konfigurieren**. Geben Sie in das Dialogfeld **SMTP-Einstellungen konfigurieren** Folgendes ein:

   a) Geben Sie in das Textfeld **Serveradresse** den Hostnamen oder die IP-Adresse des SMTP-Servers ein.

   b) Geben Sie in das Textfeld **Absender** eine E-Mail-Adresse ein, an die nicht zustellbare Benachrichtigungen und Nicht-Zustellbarkeitsmeldungen gesendet werden können.

   c) Klicken Sie auf **Test**, um die Verbindung zu testen.

3. Klicken Sie im Bereich **Empfänger** auf **Hinzufügen**.

   Das Dialogfeld **Neuer E-Mail-Benachrichtigungsempfänger** wird angezeigt.

4. Geben Sie in das Feld **E-Mail-Adresse** die Adresse des Empfängers ein.
5. Wählen Sie im Feld **Sprache** die Sprache, in der E-Mail-Benachrichtigungen gesendet werden sollen.
6. Im Fensterbereich **Abonnements** wählen Sie unter „Warnstufe überschritten“ und „Kritische Stufe überschritten“ die E-Mail-Benachrichtigungen, die Sie an diesen Empfänger senden möchten.

8.10 Einrichten von E-Mail-Benachrichtigungen für Active Directory-Synchronisierung

Bei rollenbasierter Verwaltung müssen Sie zum Konfigurieren der Active Directory-E-Mail-Benachrichtigungen zur Synchronisierung über die Berechtigung **Systemkonfiguration** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können E-Mail-Benachrichtigungen über neue Computer und Gruppen, die bei der Synchronisierung mit Active Directory gefunden werden, an gewählte Empfänger senden lassen. Wenn Sie Computer in synchronisierten Gruppen automatisch schützen möchten,

können Sie außerdem Benachrichtigungen für das Fehlschlagen des automatischen Schutzes einrichten.

1. Wählen Sie im Menü **Extras** die Option **E-Mail-Benachrichtigungen konfigurieren**.

   Das Dialogfeld **E-Mail-Benachrichtigungen konfigurieren** wird angezeigt.

2. Wenn die SMTP-Einstellungen nicht konfiguriert wurden oder wenn Sie die Einstellungen ansehen oder ändern möchten, klicken Sie auf **Konfigurieren**.

   Geben Sie in das Dialogfeld **SMTP-Einstellungen konfigurieren** Folgendes ein:

   a) Geben Sie in das Textfeld **Serveradresse** den Hostnamen oder die IP-Adresse des SMTP-Servers ein.

   b) Geben Sie in das Textfeld **Absender** eine E-Mail-Adresse ein, an die nicht zustellbare Benachrichtigungen und Nicht-Zustellbarkeitsmeldungen gesendet werden können.

   c) Klicken Sie auf **Test**, um die Verbindung zu testen.

3. Klicken Sie im Bereich **Empfänger** auf **Hinzufügen**.

   Das Dialogfeld **Neuer E-Mail-Benachrichtigungsempfänger** wird angezeigt.

4. Geben Sie in das Feld **E-Mail-Adresse** die Adresse des Empfängers ein.
5. Wählen Sie im Feld **Sprache** die Sprache, in der E-Mail-Benachrichtigungen gesendet werden sollen.
6. Wählen Sie im Fensterbereich **Abonnements** die E-Mail-Benachrichtigungen unter „Synchronisierung mit Active Directory“, die Sie an diesen Empfänger senden möchten.

   E-Mail-Benachrichtigungen unter „Synchronisierung mit Active Directory“:

   - Neue Gruppen erkannt
   - Neue Computer erkannt
   - Automatischer Schutz nicht möglich

8.11 Konfigurieren des Windows-Ereignisprotokolls

Bei rollenbasierter Verwaltung:

- Zur Ausführung dieses Tasks ist die Berechtigung **Richtlinieneinstellung – Virenschutz und HIPS** erforderlich.
- Sie können keine Richtlinien bearbeiten, die sich nicht in Ihrer aktiven Teilverwaltungseinheit befinden.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Standardmäßig schreibt Sophos Endpoint Security and Control alle Informationen bezüglich der Erkennung und/oder Bereinigung von Viren/Spyware, verdächtigem Verhalten und verdächtigen Dateien, Adware und PUA in das Ereignisprotokoll von Windows 2000 (und aufwärts).

Dies lässt sich jedoch ändern:

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf die Antivirus- und HIPS-Richtlinie, die Sie ändern möchten.
2. Klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** auf **Benachrichtigungen**.
3. Klicken Sie im Dialogfeld **Benachrichtigungen** auf die Registerkarte **Ereignisprotokoll**.

   Standardmäßig ist das Ereignisprotokoll aktiviert. Ändern Sie diese Einstellungen gegebenenfalls.

   Ein **Scan-Fehler** liegt beispielsweise auch dann vor, wenn Sophos Endpoint Security and Control auf ein Objekt nicht zugreifen konnte.

8.12 Aktivieren/Deaktivieren von Reports an Sophos

Bei rollenbasierter Verwaltung müssen Sie zum Aktivieren/Deaktivieren von Reports an Sophos über die Berechtigung **Systemkonfiguration** verfügen. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können Sophos Enterprise Console erlauben, Reports über die Anzahl verwalteter Computer und Informationen über die Arten und Versionen von Betriebssystemen und die verwendeten Sophos Produkte jede Woche an Sophos zu senden. Sophos verwendet diese Informationen, um besseren Support zu leisten und mehr Einblicke in die Produktnutzung der Kunden zu gewinnen. Die an Sophos gesendeten Informationen über Ihre Computer identifizieren keine Personen oder spezifischen Computer. Sophos verwendet diese Informationen nicht dazu, Ihr Unternehmen zu identifizieren, es sei denn, Sie geben uns Ihren Sophos Benutzernamen und/oder Ihre E-Mail-Adresse.

Reports an Sophos sind standardmäßig aktiviert. Sie können Reports an Sophos deaktivieren, wenn Sie die Konsole über den Installations-Assistenten von Sophos Enterprise Console installieren oder aktualisieren.

Wenn Sie Reports an Sophos nach der Installation ein- oder ausschalten möchten, gehen Sie folgendermaßen vor:

1. Wählen Sie im Menü **Extras** die Option **Report an Sophos**.
2. Im Dialogfeld **Report an Sophos** können Sie an Reports an Sophos aktivieren/deaktivieren.

   - *Wenn Sie Reports an Sophos aktivieren möchten,* lesen Sie die Zustimmungserklärung und aktivieren Sie das Kontrollkästchen **Ich stimme zu**, wenn Sie mit den Bedingungen einverstanden sind.
   - *Wenn Sie Reports an Sophos deaktivieren wollen,* deaktivieren Sie das Kontrollkästchen **Ich stimme zu**.

   Wenn Sie möchten, dass der technische Support von Sophos Sie (beispielsweise bei Betriebssystems- oder Versionsproblemen) direkt kontaktiert, geben Sie Ihren Sophos Benutzernamen und/oder Ihre E-Mail-Adresse ein.

   Wenn Sie die Reports zwar aktivieren möchten, Ihre Anonymität jedoch gewahrt werden soll, geben Sie Benutzernamen oder E-Mail-Adresse nicht an.

9 Ereignisanzeige

9.1 Allgemeine Informationen

Application Control-, Data Control-, Device Control- Firewall-, Patch-Analyse-, Manipulationsschutz-, Web Control- oder Verschlüsselungs-Ereignisse auf einem Endpoint (z.B. die Firewall hat eine Anwendung blockiert) werden an Enterprise Console übertragen und können in der jeweiligen Ereignisanzeige abgerufen werden.

Die Ereignisanzeige gibt Aufschluss über Fehler im Netzwerk. Zudem können Sie gefilterte Ereignislisten erstellen: z.B. eine Liste aller Data Control-Ereignisse, die in den vergangenen 7 Tagen von einem bestimmten Benutzer ausgelöst wurden.

Im Dashboard wird die Anzahl der Computer angezeigt, deren Ereignisanzahl in den vergangenen 7 Tagen einen festgelegten Höchstwert überschritten hat. Nähere Informationen zum Festlegen des Höchstwerts finden Sie im Abschnitt *Konfigurieren des Dashboards* (Seite 56).

Sie können einstellen, dass die von Ihnen ausgewählten Empfänger bei Ereignissen benachrichtigt werden. Weitere Informationen finden Sie unter *Was sind Alerts und Benachrichtigungen?* (Seite 201).

9.2 Anzeigen von Application Control-Ereignissen

So können Sie sich Application Control-Ereignisse anzeigen lassen:

1. Klicken Sie im Menü **Ereignisse** auf **Application Control-Ereignisse**.

   Das Dialogfeld **Application Control – Ereignisanzeige** wird angezeigt.

2. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Ereignisse angezeigt werden sollen.

   Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt Ihren eigenen Zeitraum bestimmen.

3. Wenn Sie Ereignisse für einen bestimmten Benutzer oder Computer aufrufen möchten, geben Sie den entsprechenden Namen in das zugehörige Feld ein.

   Wenn Sie keine spezifischen Angaben machen, werden Ereignisse für alle Benutzer und Computer angezeigt.

   Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.

4. Wenn Sie Ereignisse für einen bestimmten Anwendungstyp aufrufen möchten, wählen Sie im Dropdown-Menü **Anwendungstyp** den Anwendungstyp aus.

   Standardmäßig werden in der Ereignisanzeige Ereignisse für alle Anwendungstypen angezeigt.

5. Klicken Sie zur Anzeige einer Ereignisliste auf **Suche**.

Sie können die Liste mit Application Control-Ereignissen in eine Datei exportieren. Mehr dazu erfahren Sie unter *Exportieren der Ereignisliste in eine Datei* (Seite 222).

9.3 Anzeige von Data Control-Ereignissen

Bei rollenbasierter Verwaltung müssen Sie zur Anzeige von Data Control-Ereignissen in Enterprise Console über die Berechtigung **Data Control-Ereignisse** verfügen. Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 17) entnehmen.

So können Sie sich Data Control-Ereignisse anzeigen lassen:

1. Klicken Sie im Menü **Ereignisse** auf **Data Control-Ereignisse**.

   Das Dialogfeld **Data Control – Ereignisanzeige** wird angezeigt.

2. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Ereignisse angezeigt werden sollen.

   Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt Ihren eigenen Zeitraum bestimmen.

3. Wenn Sie Ereignisse für einen bestimmten Benutzer, Computer oder eine bestimmte Datei aufrufen möchten, geben Sie den entsprechenden Namen in das zugehörige Feld ein.

   Wenn Sie keine spezifischen Angaben machen, werden Ereignisse für alle Benutzer, Computer und Dateien angezeigt.

   Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.

4. Wenn Sie Ereignisse für eine bestimmte Regel aufrufen möchten, wählen Sie im Dropdown-Menü **Regelname** den Regelnamen aus.

   Standardmäßig werden in der Ereignisanzeige Ereignisse für alle Regeln angezeigt.

5. Wenn Sie Ereignisse für einen bestimmten Dateityp aufrufen möchten, wählen Sie im Dropdown-Menü **Dateityp** den Dateityp aus.

   Standardmäßig werden in der Ereignisanzeige Ereignisse für alle Dateitypen angezeigt.

6. Klicken Sie zur Anzeige einer Ereignisliste auf **Suche**.

Sie können die Liste mit Data Control-Ereignissen in eine Datei exportieren. Mehr dazu erfahren Sie unter *Exportieren der Ereignisliste in eine Datei* (Seite 222).

9.4 Anzeige von Device Control-Ereignissen

So können Sie sich Device Control-Ereignisse anzeigen lassen:

1. Wählen Sie im Menü **Ereignisse** die Option **Device Control-Ereignisse**.

   Das Dialogfeld **Device Control – Ereignisanzeige** wird angezeigt.

2. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Ereignisse angezeigt werden sollen.

   Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt Ihren eigenen Zeitraum bestimmen.

3. Wenn Sie Ereignisse für einen bestimmten Gerätetyp aufrufen möchten, wählen Sie im Dropdown-Menü **Gerätetyp** den Gerätetyp aus.

   Standardmäßig werden in der Ereignisanzeige Ereignisse für alle Gerätetypen angezeigt.

4. Wenn Sie Ereignisse für einen bestimmten Benutzer oder Computer aufrufen möchten, geben Sie den entsprechenden Namen in das zugehörige Feld ein.

   Wenn Sie keine spezifischen Angaben machen, werden Ereignisse für alle Benutzer und Computer angezeigt.

   Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.

5. Klicken Sie zur Anzeige einer Ereignisliste auf **Suche**.

Im Dialogfeld **Device Control – Ereignisanzeige** können Sie ein Gerät von Device Control-Richtlinien ausschließen. Mehr dazu erfahren Sie unter *Ausschließen eines Geräts von allen Richtlinien* (Seite 176).

Sie können die Liste von Device Control-Ereignissen in eine Datei exportieren. Mehr dazu erfahren Sie unter *Exportieren der Ereignisliste in eine Datei* (Seite 222).

9.5 Anzeige von Firewall-Ereignissen

Firewall-Ereignisse werden nur einmal von einem Computer an die Konsole gesendet. Identische Ereignisse von verschiedenen Computern werden in der **Firewall – Ereignisanzeige** gruppiert. In der Spalte **Anzahl** wird angezeigt, wie häufig ein Ereignis von diversen Endpoints gesendet wurde.

So werden Firewall-Ereignisse angezeigt:

1. Klicken Sie im Menü **Ereignisse** auf **Firewall-Ereignisse**.

   Das Dialogfeld **Firewall – Ereignisanzeige** wird angezeigt.

2. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Ereignisse angezeigt werden sollen.

   Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt Ihren eigenen Zeitraum bestimmen.

3. Wenn Sie Ereignisse eines bestimmten Typs aufrufen möchten, wählen Sie den gewünschten Typ im Dropdown-Menü **Ereignistyp** aus.

   Standardmäßig werden in der Ereignisanzeige Ereignisse für alle Typen angezeigt.

4. Wenn Sie Ereignisse für eine bestimmte Datei aufrufen möchten, geben Sie in das Feld **Dateiname** den entsprechenden Namen ein.

   Wenn Sie keine spezifischen Angaben machen, werden Ereignisse für alle Dateien angezeigt.

   Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.

5. Klicken Sie zur Anzeige einer Ereignisliste auf **Suche**.

Im Dialogfeld **Firewall – Ereignisanzeige** können Sie anhand der Anweisungen im Abschnitt *Erstellen einer Firewall-Ereignisregel* (Seite 122) eine Firewall-Regel erstellen.

Sie können die Liste mit Firewall-Ereignissen in eine Datei exportieren. Mehr dazu erfahren Sie unter *Exportieren der Ereignisliste in eine Datei* (Seite 222).

9.6 Anzeige von Verschlüsselungsereignissen

So können Sie zu von der Festplattenverschlüsselung protokollierte Ereignisse aufrufen:

1. Klicken Sie im Menü **Ereignisse** auf **Verschlüsselungsereignisse**.

   Das Dialogfeld **Verschlüsselungsereignisse – Ereignisanzeige** wird angezeigt.

2. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Ereignisse angezeigt werden sollen.

   Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt Ihren eigenen Zeitraum bestimmen.

3. Wenn Sie Ereignisse für einen bestimmten Benutzer oder Computer aufrufen möchten, geben Sie den entsprechenden Namen in das zugehörige Feld ein.

   Wenn Sie keine spezifischen Angaben machen, werden Ereignisse für alle Benutzer und Computer angezeigt.

   Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.

4. Wenn Sie Ereignisse einer bestimmten Ebene aufrufen möchten, wählen Sie den gewünschten Typ im Dropdown-Menü **Ebene** aus. **Alle**, **Fehler** oder **Warnung**.

   Standardmäßig werden in der Ereignisanzeige Ereignisse für alle Ebenen angezeigt.

5. Klicken Sie zur Anzeige einer Ereignisliste auf **Suche**.

Sie können die Ereignisliste in eine Datei exportieren. Mehr dazu erfahren Sie unter *Exportieren der Ereignisliste in eine Datei* (Seite 222).

Hinweis: Auf dem Endpoint werden alle Ereignisse protokolliert. Sie können diese im Ereignisprotokoll von Windows abrufen.

9.7 Anzeige von Manipulationsschutz-Ereignissen

Es wird zwischen den folgenden Manipulationsschutz-Ereignissen unterschieden:

- Erfolgreiche Manipulationsschutz-Ereignisse (Anzeige des Namens des authentifizierten Benutzers sowie des Authentifizierungszeitpunkts).
- Nicht erfolgreiche Manipulationsschutz-Ereignisse (Anzeige des Zielprodukts/der Zielkomponente, des Manipulationszeitpunkts und der Daten des Benutzers, der den Manipulationsversuch unternommen hat).

So können Sie sich Manipulationsschutz-Ereignisse anzeigen lassen:

1. Klicken Sie im Menü **Ereignisse** auf **Manipulationsschutz-Ereignisse**.

   Das Dialogfeld **Manipulationsschutz – Ereignisanzeige** wird angezeigt.

2. Wählen Sie im Dropdown-Menü **Suchperiode** den Zeitraum aus, für den Ereignisse angezeigt werden sollen.

   Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt Ihren eigenen Zeitraum bestimmen.

3. Wenn Sie Ereignisse eines bestimmten Typs aufrufen möchten, wählen Sie den gewünschten Typ im Dropdown-Menü **Ereignistyp** aus.

   Standardmäßig werden in der Ereignisanzeige Ereignisse für alle Typen angezeigt.

4. Wenn Sie Ereignisse für einen bestimmten Benutzer oder Computer aufrufen möchten, geben Sie den entsprechenden Namen in das zugehörige Feld ein.

   Wenn Sie keine spezifischen Angaben machen, werden Ereignisse für alle Benutzer und Computer angezeigt.

   Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.

5. Klicken Sie zur Anzeige einer Ereignisliste auf **Suche**.

Sie können die Ereignisliste in eine Datei exportieren. Mehr dazu erfahren Sie unter *Exportieren der Ereignisliste in eine Datei* (Seite 222).

9.8 Anzeige der Patch-Analyse-Ereignisse

9.8.1 Informationen zur Patch-Analyse-Ereignisanzeige

In der „**Patch-Analyse – Ereignisanzeige**“ werden Informationen zu Sicherheits-Patches sowie die Ergebnisse der Patch-Analyse aufgeführt.

Im Feld **Patch-Updates** wird der Downloadstatus von Patchinformationen angezeigt. Eine der folgenden Statusmeldungen wird angezeigt:

- **Nicht heruntergeladen** weist darauf hin, dass Patchinformationen nicht heruntergeladen wurden oder die Patch-Funktion nicht im Lizenzumfang enthalten ist.

- **Download läuft** weist darauf hin, dass der erste Download nach der Installation ausgeführt wird.
- **OK** zeigt an, dass sich die Patchinformationen auf dem neuesten Stand befinden.
- **Nicht auf dem neuesten Stand** weist darauf hin, dass die Patch-Daten in den letzten 72 Stunden nicht erfolgreich upgedatet wurden. Der Status wird in der Regel angezeigt, wenn sich SEC aufgrund von Netzwerkproblemen nicht auf dem neuesten Stand befindet. Unter Umständen wird er auch bei der Umstellung von einer Lizenz von SEC mit Patch-Funktion zu einer ohne angezeigt. Unter Umständen wurde bei Anzeige der Statusmeldung ein Teil-Update durchgeführt.

Die „**Patch-Analyse – Ereignisanzeige**“ verfügt über die folgenden Registerkarten:

Patches nach Bewertung

Auf der Registerkarte werden standardmäßig fehlende Patches angezeigt. Alle Patches und die dazugehörigen Threats und Sicherheitslücken werden angezeigt. Zudem wird angegeben, auf wie vielen Computern Patches fehlen. Anhand von Filtern können Sie eine Liste aller unterstützten Patches anzeigen sowie die Anzahl der Computer, auf denen sie fehlen.

Computer mit fehlenden Patches

In der Registerkarte wird der Patch-Analysestatus nach Computer angezeigt. Es werden alle Computer und die jeweiligen fehlenden Patches angezeigt. Wenn mehrere Patches fehlen, erscheinen die Computer mehrmals in der Liste.

9.8.2 Anzeige der Patch-Analyse-Ereignisse

So können Sie die Patch-Analyse-Ereignisse aufrufen:

1. Wählen Sie im Menü **Ereignisse** die Option **Patch-Analyse-Ereignisse**.

   Das Dialogfeld **Patch-Analyse – Ereignisanzeige** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Patches nach Bewertung** oder **Computer mit fehlenden Patches**. Nähere Informationen zu Registerkarten finden Sie unter *Informationen zur Patch-Analyse-Ereignisanzeige* (Seite 216).
3. Wenn Sie Ereignisse zu einem bestimmten Patch, Namen, Computer, Threat oder einer Sicherheitslücke abrufen möchten, geben Sie im Suchfeld die erforderlichen Daten ein. Die Suchkriterien variieren in Abhängigkeit der in der Registerkarte angezeigten Informationen.

   Wenn Sie keine spezifischen Angaben machen, werden Ereignisse für alle Patch-Namen, Patch-IDs und Computernamen angezeigt.

   Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.
4. Wenn Sie Ereignisse zu einem bestimmten Patch-Status, einer Bewertung, einem Hersteller, einer Gruppe oder einem Veröffentlichungsdatum aufrufen möchten, klicken Sie auf den Dropdown-Pfeil und wählen Sie die passende Option aus. Die Suchkriterien variieren in Abhängigkeit der in der Registerkarte angezeigten Informationen.

   Standardmäßig werden Ereignisse für Threat-Bewertungen, Hersteller, Gruppen, Threats und Patch-Namen für fehlende Patches angezeigt.

5. Klicken Sie zur Anzeige einer Liste mit Patch-Analyse-Ereignissen auf **Suche**.

   Nähere Informationen zu den Ergebnissen finden Sie unter *Kategorien der Suchergebnisse* (Seite 219).

Sie können auf einen Hyperlink rechtsklicken und so den Namen des Links kopieren oder eine Patch-Analyse-Zeile mit „Strg“ + „C“ in die Zwischenablage kopieren.

Sie können die Liste mit den Patch-Analyse-Ereignissen exportieren. Mehr dazu erfahren Sie unter *Exportieren der Ereignisliste in eine Datei* (Seite 222).

Klicken Sie auf den Link, um Details zu einem bestimmten Patch anzuzeigen. Nähere Informationen finden Sie unter *Anzeige von Patch-, Threat und Sicherheitslückeninformationen* (Seite 218).

9.8.3 Anzeige von Patch-, Threat und Sicherheitslückeninformationen

So können Sie Informationen zu Patches, Threats und Sicherheitslücken abrufen:

1. Wählen Sie im Menü **Ereignisse** die Option **Patch-Analyse-Ereignisse**.

   Das Dialogfeld **Patch-Analyse – Ereignisanzeige** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Patches nach Bewertung** oder **Computer mit fehlenden Patches**, wählen Sie die erforderliche Option aus, und klicken Sie auf **Suche**, um eine Ergebnisliste anzuzeigen.

   Nähere Informationen zu den Ergebnissen finden Sie unter *Kategorien der Suchergebnisse* (Seite 219).

3. Klicken Sie auf den Patch-Namen, zu dem Details angezeigt werden sollen.
4. Im Dialogfeld **Patch-Detail** wird der Patch näher beschrieben. Zudem finden Sie hier die Threats und Sicherheitslücken, vor denen der Patch schützt. Falls vorhanden, bieten sich folgende Optionen:

   - Klicken Sie auf den Patch-Namen. Ein Browserfenster mit Herstellerinformation zu einem bestimmten Patch öffnet sich.
   - Klicken Sie auf den Threat. Ein Browserfenster mit den Threat-Analysen sowie Empfehlungen von Sophos öffnet sich.
   - Klicken Sie auf die Sicherheitslücke. Ein Browserfenster mit CVE-Informationen (Common vulnerabilities and exposures) öffnet sich.
   - Klicken Sie auf den Patch-Namen in der Spalte **Vorgänger**, um ein Browserfenster mit Informationen zum Hersteller eines abgelösten Patches aufzurufen.

Die Liste ist alphabetisch nach Threat und Sicherheitslücke geordnet.

9.8.4 Suchergebnisse der Patch-Analyse

9.8.4.1 Kategorien der Suchergebnisse

Die Suchergebnisse werden je nach Registerkarte in unterschiedlichen Kategorien angezeigt:

- *Patches nach Bewertung* (Seite 219)
- *Computer mit fehlenden Patches* (Seite 220)

9.8.4.2 Patches nach Bewertung

Die Suchergebnisse werden anhand der folgenden Kategorien angeordnet:

- **Threats**: Bei Threats handelt es sich um Viren, Trojaner, Würmer, Spyware, schädliche Websites, Adware oder sonstige potenziell unerwünschte Anwendungen. Sie können auf den Threat-Namen klicken, um die Threat-Analyse von Sophos und Empfehlungen im Web-Browser aufzurufen.
- **Sicherheitslücken**: Sicherheitslücken sind Schwachstellen in Software, die von Angreifern ausgenutzt werden können. Der Schaden, der vom Ausnutzen einer Sicherheitslücke verursacht werden kann, hängt von der jeweiligen Sicherheitslücke und der betroffenen Software ab. Patches sorgen dafür, dass Sicherheitslücken nicht mehr ausgenutzt werden können. Sie können auf den Namen der Sicherheitslücke klicken, um die CVE-Daten im Web-Browser aufzurufen.
- **Bewertung**: Die Patches werden von den SophosLabs bewertet.

  Hinweis: Es empfiehlt sich, Patches ungeachtet der Bewertung zu installieren.

  - **Kritisch**: Es ist davon auszugehen, dass diese Sicherheitslücke(n) ausgenutzt wird/werden.
  - **Hoch**: Die Wahrscheinlichkeit, dass die Sicherheitslücke(n) ausgenutzt wird/werden, ist hoch.
  - **Mittelschwer**: Es ist möglich, dass die Sicherheitslücke(n) ausgenutzt wird/werden.
  - **Niedrig**: Die Wahrscheinlichkeit, dass die Sicherheitslücke(n) ausgenutzt wird/werden, ist gering.

- **Patch-Name**: Der Name des Patches wird angezeigt. Sie können auf den Patch-Namen klicken, um ein Browserfenster mit Herstellerinformation zu einem bestimmten Patch zu öffnen.
- **Herstellerr**: Der Name des Herstellers, der den Patch veröffentlicht hat, wird angezeigt.
- **Computer**: Die Anzahl der betroffenen Computer wird angezeigt. Wenn einer oder mehrere Computer betroffen sind, können Sie auf die Anzahl klicken, um Details in der Registerkarte **Computer mit fehlenden Patches** abzurufen. Ein „-“ weist darauf hin, dass der Patch nicht analysiert wird.
- **Abgelöst von**: Die Namen der abgelösten Patches werden angezeigt. Sie können zum Öffnen des Dialogfelds **Patch-Detail** auf den Patch-Namen klicken und so Informationen zu den abgelösten Patches abrufen.

- **Veröffentlichungsdatum**: Das Datum, an dem der Patch veröffentlicht wurde, wird angezeigt.

9.8.4.3 Computer mit fehlenden Patches

Die Suchergebnisse werden anhand der folgenden Kategorien angezeigt:

- **Computer**: Der Name des betroffenen Computers wird angezeigt.
- **Bewertung**: Die Patches werden von den SophosLabs bewertet.

  Hinweis: Es empfiehlt sich, Patches ungeachtet der Bewertung zu installieren.

  - **Kritisch**: Es ist davon auszugehen, dass diese Sicherheitslücke(n) ausgenutzt wird/werden.
  - **Hoch**: Die Wahrscheinlichkeit, dass die Sicherheitslücke(n) ausgenutzt wird/werden, ist hoch.
  - **Mittelschwer**: Es ist möglich, dass die Sicherheitslücke(n) ausgenutzt wird/werden.
  - **Niedrig**: Die Wahrscheinlichkeit, dass die Sicherheitslücke(n) ausgenutzt wird/werden, ist gering.

- **Patch-Name**: Der Name des Patches wird angezeigt. Sie können auf den Patch-Namen klicken, um ein Browserfenster mit Herstellerinformation zu einem bestimmten Patch zu öffnen.
- **Abgelöst von**: Die Namen der abgelösten Patches werden angezeigt. Sie können zum Öffnen des Dialogfelds **Patch-Detail** auf den Patch-Namen klicken und so Informationen zu den abgelösten Patches abrufen.
- **Letzte Analyse**: Das Datum der letzten Überprüfung auf fehlende Patches wird angezeigt.
- **Herstellerr**: Der Name des Herstellers, der den Patch veröffentlicht hat, wird angezeigt.
- **Veröffentlichungsdatum**: Das Datum, an dem der Patch veröffentlicht wurde, wird angezeigt.
- **Gruppe**: Der Name der Gruppe, der der Computer angehört, wird angezeigt.

9.9 Anzeige von Web-Ereignissen

9.9.1 Anzeige von Web-Ereignissen

Bei rollenbasierter Verwaltung müssen Sie zur Anzeige von Web-Ereignissen in Enterprise Console über die Berechtigung **Web-Ereignisse** verfügen. Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 17) entnehmen.

Sie können die folgenden Web-Ereignisse in der Web-Ereignisanzeige abrufen:

- Vom Web-Schutz in der **Antivirus- und HIPS**-Richtlinie gesperrte Seiten.
- Web Control-Ereignisse (bei Nutzung von Web Control).

Die Anzeige von Web Control-Ereignissen variiert in Abhängigkeit der gewählten Web Control-Richtlinie. Zwar unterstützt die Web-Ereignisanzeige beide Richtlinienmodi, die Inhalte unterscheiden sich jedoch.

Bei Auswahl der Option **Kontrolle unangebrachter Websites** werden sämtliche „Blockier"- und „Warn"-Vorgänge angezeigt. Aufgerufene HTTPS-Sites in der „Warn"-Kategorie werden als „Fortsetzen"-Ereignisse protokolliert, da Sophos Endpoint Security and Control anders auf HTTPS reagiert (siehe Hinweis im Abschnitt *Informationen zur Kontrolle unangebrachter Websites* (Seite 193)).

Bei Auswahl der umfasenden **Web Control**-Funktion werden Ereignisse auf der Sophos Web Appliance oder Management Appliance angezeigt. Die Funktionen **Reports** und **Suche** gibt Aufschluss über die Browser-Aktivität. Die Maßnahmen „Blockieren", „Warnen" und „Zulassen" werden angezeigt. Aufgerufene HTTPS-Sites in der „Warn"-Kategorie werden als „Fortsetzen"-Ereignisse angezeigt, da Sophos Endpoint Security and Control anders auf HTTPS reagiert (siehe Hinweis im Abschnitt *Vollständige Web Control* (Seite 198)).

Hinweis: Ungeachtet der gewählten Richtlinie werden von der Live-URL-Filterfunktion (Web-Schutz) in Sophos Endpoint Security and Control gescannte Websites in Enterprise Console als Web-Ereignisse angezeigt.

So werden Web-Ereignisse angezeigt:

1. Klicken Sie im Menü **Ereignisse** auf **Web-Ereignisse**.

   Das Dialogfeld **Web – Ereignisanzeige** wird angezeigt.

2. Wählen Sie im Feld **Suchperiode** den Zeitraum aus, für den Ereignisse angezeigt werden sollen.

   Sie können einen festen Zeitraum, etwa **24 Std.**, festlegen oder über die Option **Benutzerdefiniert** durch Auswahl von Start- und Endzeitpunkt Ihren eigenen Zeitraum bestimmen.

3. Wenn Sie Ereignisse für einen bestimmten **Benutzer** oder **Computer** aufrufen möchten, geben Sie den entsprechenden Namen in das zugehörige Feld ein.

   Wenn Sie keine spezifischen Angaben machen, werden Ereignisse für alle Benutzer und Computer angezeigt.

   Die Eingabe folgender Platzhalter ist erlaubt: ? für ein einzelnes Zeichen und * für eine Zeichenfolge.

4. Wenn Sie Ereignisse in Zusammenhang mit einer bestimmten Maßnahme aufrufen möchten, wählen Sie die Maßnahme im Dropdown-Menü **Maßnahme** aus.
5. Wenn Sie Ereignisse in Zusammenhang mit einer bestimmten Domäne anzeigen möchten, geben Sie sie in das Feld **Domäne** ein.
6. Wenn Sie Ereignisse anzeigen möchten, die aus einem bestimmten **Grund** erfolgt sind, klicken Sie auf den Dropdown-Pfeil und wählen Sie einen Grund aus.
7. Klicken Sie zur Anzeige einer Ereignisliste auf **Suche**.

Sie können die Liste von Web-Ereignissen in eine Datei exportieren. Mehr dazu erfahren Sie unter *Exportieren der Ereignisliste in eine Datei* (Seite 222).

9.9.2 Anzeige der aktuellen Web-Ereignisse auf einem Computer

Sie können die letzten 10 Ereignisse zu einer auf einem Endpoint vorgenommenen Maßnahme (z.B. gerade gesperrte Websites) anzeigen.

So können Sie die aktuellen Web-Ereignisse aufrufen:

1. Doppelklicken Sie in der Ansicht **Endpoints** in der Computerliste auf den Computer, dessen Web-Aktivität angezeigt werden sollen.
2. Navigieren Sie im Dialogfeld **Computer-Details** zu **Aktuelle Web-Ereignisse**.

Sie können auch einen Report erstellen, aus dem die Anzahl der Ereignisse für einen bestimmten Benutzer hervorgeht. Weitere Informationen finden Sie unter *Konfigurieren des Reports „Ereignisse nach Benutzer“* (Seite 230).

9.10 Exportieren der Ereignisliste in eine Datei

Sie können Application Control-, Firewall-, Data Control- , Device Control-, Patch-Analyse-, Verschlüsselungs-, Manipulationsschutz- oder Web-Ereignisse in eine CSV-Datei exportieren. Sie können die Liste mit den Patch-Analyse-Ereignissen auch in eine PDF-Datei exportieren.

1. Klicken Sie im Menü **Ereignisse** auf die „Ereignis“-Option, die der zu exportierenden Liste entspricht.

   Das Dialogfeld **Ereignisanzeige** wird angezeigt.

2. Wenn nur ausgewählte Ereignisse angezeigt werden sollen, legen Sie im Feld **Suchkriterien** Filter fest und klicken Sie zur Anzeige der Ereignisse auf **Suchen**.

   Weitere Informationen erhalten Sie unter *Anzeigen von Application Control-Ereignissen* (Seite 212), *Anzeige von Data Control-Ereignissen* (Seite 213), *Anzeige von Device Control-Ereignissen* (Seite 213), *Anzeige von Verschlüsselungsereignissen* (Seite 215), *Anzeige von Firewall-Ereignissen* (Seite 214), *Anzeige der Patch-Analyse-Ereignisse* (Seite 217), *Anzeige von Manipulationsschutz-Ereignissen* (Seite 216) oder *Anzeige von Web-Ereignissen* (Seite 220).

3. Klicken Sie auf **Exportieren**.
4. Geben Sie im Fenster **Speichern unter** ein Zielverzeichnis an, geben Sie im Feld **Dateiname** einen Namen und wählen Sie einen Dateityp im Feld **Dateityp** aus.
5. Klicken Sie auf **Speichern**.

10 Erstellen von Reports

10.1 Reports

Reports liefern Informationen (in Form von Text und Grafiken) zu diversen Aspekten der Netzwerksicherheit.

Reports können Sie im **Report Manager** aufrufen. Mit dem **Report Manager** können Sie auf der Basis vorhandener Vorlagen schnell Reports erstellen, die Konfiguration eines Reports ändern und die Reporterstellung zeitlich planen. Die Reportergebisse werden den gewählten Empfängern als E-Mail-Anhang zugesandt. Sie können Reports ausdrucken und in unterschiedlichen Formaten exportieren.

Sophos bietet vordefinierte Reports, die Sie nach Belieben an Ihre Bedürfnisse anpassen können. Folgende Reports sind vorhanden:

- Alert- und Ereignisverlauf
- Alert-Übersicht
- Alerts und Ereignisse nach Objektname
- Alerts und Ereignisse nach Zeit
- Alerts und Ereignisse nach Ort
- Endpoint-Richtlinienabweichung
- Ereignisse nach Benutzer
- Schutz verwalteter Endpoints
- Update-Hierarchie

Reports und rollenbasierte Administration

Bei rollenbasierter Administration müssen Sie zum Erstellen, Bearbeiten und Löschen von Reports über die Berechtigung **Report-Konfiguration** verfügen. Wenn Sie die Berechtigung nicht besitzen, können Sie Reports lediglich ausführen. Nähere Informationen zur rollenbasierten Verwaltung können Sie dem Abschnitt *Rollen und Teilverwaltungseinheiten* (Seite 17) entnehmen.

Reports können nur Daten aus der aktiven Teilverwaltungseinheit umfassen. Sie können Reports nicht auf andere Teilverwaltungseinheiten übertragen. Die Standardreports werden nicht von der Teilverwaltungseinheit **Standard** in neu erstellte Teilverwaltungseinheiten kopiert.

Beim Löschen einer Teilverwaltungseinheit gehen auch die darin enthaltenen Reports verloren.

10.2 Erstellen eines neuen Reports

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

So können Sie einen Report erstellen:

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Klicken Sie im Dialogfeld **Report Manager** auf **Erstellen**.
3. Wählen Sie im Dialogfeld **Neuen Report erstellen** eine Report-Vorlage aus und klicken Sie auf **OK**.

   Ein Assistent leitet Sie durch die Report-Erstellung und richtet sich dabei nach der gewählten Vorlage.

   Wenn Sie den Assistenten nicht verwenden möchten, deaktivieren Sie im Dialogfeld **Neuer Report** die Option **Report mit Assistent erstellen**. Sie können den neuen Report im Dialogfeld „Report-Eigenschaften“ konfigurieren. Nähere Informationen finden Sie in den Abschnitten, die den jeweiligen Report thematisieren.

10.3 Konfigurieren des Reports „Alert- und Ereignisverlauf“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Im Report **Alert- und Ereignisverlauf** werden alle Alerts und Ereignisse in einem bestimmten Zeitraum angezeigt.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Alert- und Ereignisverlauf** aus und klicken Sie auf **Eigenschaften**.
3. Rufen Sie im Dialogfeld **Alert- und Ereignisverlauf – Eigenschaften** die Registerkarte **Konfiguration** auf und nehmen Sie die gewünschten Einstellungen vor.

   a) Im Fenster **Report-Details** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.

   b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.

      Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.

   c) Klicken Sie im Dialogfeld **Erfassungsbereich** auf **Computergruppe** oder **Einzelcomputer**. Klicken Sie dann auf den Dropdown-Pfeil, um eine Gruppe oder einen Computernamen anzugeben.

   d) Wählen Sie im Fenster **Einzubeziehende Alerts und Ereignisse** die Alert- und Ereignis-Arten aus, die von dem Report erfasst werden sollen.

      Standardmäßig berücksichtigt der Report alle Alert- und Ereignis-Arten.

      Sie können den Report auch so konfigurieren, dass nur Orte angegeben werden, für die ein bestimmter Alert oder ein Ereignis gemeldet wurde. Klicken Sie hierzu auf **Erweitert** und klicken Sie auf einen Alert- oder und Ereignisnamen in der Liste. Wenn Sie mehrere Alerts oder Ereignisse angeben möchten, tragen Sie unter Verwendung von Platzhaltern einen Namen in das Textfeld ein. ? steht für ein einzelnes Zeichen im Namen und * für

eine Zeichenfolge. Zum Beispiel steht W32/* für alle Viren, deren Namen mit W32/ beginnen.

4. Wählen Sie auf der Registerkarte **Anzeigeoptionen** die gewünschte Sortieroption für die Alerts und Ereignisse aus.

   Standardmäßig werden Alerts und Ereignisse nach **Namen** sortiert. Reports können jedoch auch nach **Computernamen**, **Gruppennamen** oder **Zeitstempel** angeordnet werden.

5. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

10.4 Konfigurieren des Reports „Alert-Übersicht“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Der Report **Alert-Übersicht** liefert statistische Informationen über den allgemeinen Netzwerkszustand.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Alert-Übersicht** aus und klicken Sie auf **Eigenschaften**.
3. Wählen Sie im Dialogfeld **Alert-Übersicht – Eigenschaften** auf der Registerkarte **Konfiguration** die gewünschten Optionen aus.

   a) Im Fenster **Report-Details** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.

   b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.

      Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.

4. Geben Sie auf der Registerkarte **Anzeigeoptionen** unter **Häufigkeit der Ergebnisanzeige** an, wie oft Nichtkonformität festgestellt werden soll (z.B. jede Stunde oder jeden Tag). Klicken Sie auf den Dropdown-Pfeil und wählen Sie ein Intervall aus.
5. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

10.5 Konfigurieren des Reports „Alerts und Ereignisse nach Objektname“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Der Report **Alerts nach Objekt** liefert statistische Informationen zu allen Alerts und Ereignissen, die auf allen Computern in einem festgelegten Zeitraum angezeigt wurden. Die Alerts sind nach dem Objektnamen sortiert.

So können Sie den Report konfigurieren:

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Alerts und Ereignisse nach Objektname** aus und klicken Sie auf **Eigenschaften**.
3. Rufen Sie im Dialogfeld **Alerts und Ereignisse nach Objektname – Eigenschaften** die Registerkarte **Konfiguration** auf und nehmen Sie die gewünschten Einstellungen vor.

   a) Im Fenster **Report-Details** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.

   b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.

   Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.

   c) Klicken Sie im Dialogfeld **Erfassungsbereich** auf **Computergruppe** oder **Einzelcomputer**. Klicken Sie dann auf den Dropdown-Pfeil, um eine Gruppe oder einen Computernamen anzugeben.

   d) Wählen Sie im Fenster **Einzubeziehende Alerts und Ereignisse** die Alert- und Ereignis-Arten aus, die von dem Report erfasst werden sollen.

   Standardmäßig berücksichtigt der Report alle Alert- und Ereignis-Arten.

4. Wählen Sie auf der Registerkarte **Anzeige-Optionen** unter **Anzeige** die Alerts und Ereignisse aus, die im Report aufgeführt werden sollen.

   Standardmäßig zeigt der Report alle Alerts und Ereignisse und deren Häufigkeit an.

   Sie können den Report auch dazu konfigurieren, nur Folgendes anzuzeigen:

   - die ersten *n* Alerts und Ereignisse (wobei *n* eine von Ihnen festgelegte Anzahl ist) oder
   - Alerts und Ereignisse mit mindestens *m* Vorkommnissen (wobei *m* eine von Ihnen festgelegte Anzahl ist).

5. Wählen Sie unter **Sortieren nach** aus, ob Alerts und Ereignisse nach Häufigkeit oder Name sortiert werden sollen.

   Als Standard listet der Report Alerts und Ereignisse in absteigender Reihenfolge nach ihrer Häufigkeit auf.

6. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

10.6 Konfigurieren des Reports „Alerts und Ereignisse nach Zeit“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Im Report **Alerts nach Zeit** werden Alerts und Ereignisse in regelmäßigen Abständen zusammengefasst.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Alerts und Ereignisse nach Zeit** aus und klicken Sie auf **Eigenschaften**.
3. Rufen Sie im Dialogfeld **Alerts und Ereignisse nach Zeit – Eigenschaften** die Registerkarte **Konfiguration** auf und nehmen Sie die gewünschten Einstellungen vor.

   a) Im Fenster **Report-Details** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.

   b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.

   Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.

   c) Klicken Sie im Dialogfeld **Erfassungsbereich** auf **Computergruppe** oder **Einzelcomputer**. Klicken Sie dann auf den Dropdown-Pfeil, um eine Gruppe oder einen Computernamen anzugeben.

   d) Wählen Sie im Fenster **Einzubeziehende Alerts und Ereignisse** die Alert- und Ereignis-Arten aus, die von dem Report erfasst werden sollen.

   Standardmäßig berücksichtigt der Report alle Alert- und Ereignis-Arten.

   Sie können den Report auch so konfigurieren, dass nur Orte angegeben werden, für die ein bestimmter Alert oder ein Ereignis gemeldet wurde. Klicken Sie hierzu auf **Erweitert** und klicken Sie auf einen Alert- oder und Ereignisnamen in der Liste. Wenn Sie mehrere Alerts oder Ereignisse angeben möchten, tragen Sie unter Verwendung von Platzhaltern einen Namen in das Textfeld ein. ? steht für ein einzelnes Zeichen im Namen und * für eine Zeichenfolge. Zum Beispiel steht W32/* für alle Viren, deren Namen mit W32/ beginnen.

4. Geben Sie auf der Registerkarte **Anzeigeoptionen** Zeitintervalle an, in denen die Häufigkeit von Alerts und Ereignissen gemessen wird, z.B. jede Stunde oder jeden Tag, klicken Sie auf den Dropdown-Pfeil und wählen ein Intervall aus.

5. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

10.7 Konfigurieren des Reports „Alerts und Ereignisse nach Ort“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Der Report **Alerts nach Ort und Ereignissen** liefert statistische Informationen zu allen Alerts, die auf allen Computern in einem festgelegten Zeitraum angezeigt wurden. Die Alerts sind nach dem Ort sortiert.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Alerts nach Ort und Ereignissen** aus und klicken Sie auf **Eigenschaften**.
3. Rufen Sie im Dialogfeld **Alerts und Ereignisse nach Ort – Eigenschaften** die Registerkarte **Konfiguration** auf und nehmen Sie die gewünschten Einstellungen vor.

   a) Im Fenster **Report-Details** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.

   b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.

   Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.

   c) Klicken Sie im Fenster **Report-Verzeichnis** auf **Computer**, um sich die Alerts pro Computer anzeigen zu lassen oder auf **Gruppe**, um sich die Alerts für jede Computergruppe anzeigen zu lassen.

   d) Wählen Sie im Fenster **Einzubeziehende Alerts und Ereignisse** die Alert- und Ereignis-Arten aus, die von dem Report erfasst werden sollen.

   Standardmäßig berücksichtigt der Report alle Alert- und Ereignis-Arten.

   Sie können den Report auch so konfigurieren, dass nur Orte angegeben werden, für die ein bestimmter Alert oder ein Ereignis gemeldet wurde. Klicken Sie hierzu auf **Erweitert** und klicken Sie auf einen Alert- oder und Ereignisnamen in der Liste. Wenn Sie mehrere Alerts oder Ereignisse angeben möchten, tragen Sie unter Verwendung von Platzhaltern einen Namen in das Textfeld ein. ? steht für ein einzelnes Zeichen im Namen und * für eine Zeichenfolge. Zum Beispiel steht W32/* für alle Viren, deren Namen mit W32/ beginnen.

4. Wählen Sie auf der Registerkarte **Anzeige-Optionen** unter **Anzeige** die Orte aus, die im Report aufgeführt werden sollen.

   Standardmäßig zeigt der Report alle Computer und Gruppen und die Häufigkeit der jeweiligen Alerts an. Sie können den Report aber auch so konfigurieren, dass nur Folgendes angezeigt wird:

   - die obersten *n* Orte, für die die meisten Alerts und Ereignisse verzeichnet wurden (wobei *n* eine von Ihnen festgelegte Anzahl ist) oder
   - Orte, die *m* Mal oder öfter vorkommen (wobei *m* eine von Ihnen festgelegte Anzahl ist)

5. Wählen Sie unter **Sortieren nach** aus, ob Sie die Orte nach der Anzahl der erkannten Objekte oder nach Namen sortieren möchten.

   Als Standard listet der Report die Orte absteigend nach der Anzahl der Alerts und Ereignisse pro Ort auf. Markieren Sie den **Ort**, wenn die erkannten Objekte alphabetisch nach Namen sortiert werden sollen.

6. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

10.8 Konfigurieren des Reports „Endpoint-Richtlinienabweichung“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Im Report **Endpoint-Richtlinienabweichung** wird der prozentuale Anteil oder die Anzahl der Computer, die nicht mit der Gruppenlichtlinie konform sind, in regelmäßigen Abständen zusammengefasst.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Endpoint-Richtlinienabweichung** aus und klicken Sie auf **Eigenschaften**.
3. Wählen Sie im Dialogfeld **Endpoint-Richtlinienabweichung – Eigenschaften** auf der Registerkarte **Konfiguration** die gewünschten Optionen aus.

   a) Im Fenster **Report-Details** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.

   b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.

   Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.

   c) Wählen Sie im Fenster **Anzeigen** die Richtlinien aus, die im Report aufgeführt werden sollen. Standardmäßig ist nur die **Anti-Virus- und HIPS**-Richtlinie ausgewählt.

4. Geben Sie auf der Registerkarte **Anzeigeoptionen** unter **Häufigkeit der Ergebnisanzeige** an, wie oft Nichtkonformität festgestellt werden soll (z.B. jede Stunde oder jeden Tag). Klicken Sie auf den Dropdown-Pfeil und wählen Sie ein Intervall aus.
5. Wählen Sie im Bereich **Ergebnisse anzeigen als**, ob die Ergebnisse prozentual oder in Zahlen angezeigt werden sollen.
6. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

10.9 Konfigurieren des Reports „Ereignisse nach Benutzer“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Im Report **Ereignisse nach Benutzer** werden Application Control-, Firewall-, Data Control- und Device Control-Ereignisse sowie Web-Ereignisse nach Benutzer gruppiert.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Ereignisse nach Benutzer** aus und klicken Sie auf **Eigenschaften**.
3. Rufen Sie im Dialogfeld **Ereignisse nach Benutzer – Eigenschaften** die Registerkarte **Konfiguration** auf und nehmen Sie die gewünschten Einstellungen vor.

   a) Im Fenster **Report-Details** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.

   b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.

   Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.

   c) Wählen Sie im Bereich **Einzubeziehende Ereignisse** die Funktionen aus, für die Ereignisse angezeigt werden sollen.

4. Wählen Sie auf der Registerkarte **Anzeige-Optionen** unter **Anzeige** die Benutzer aus, die im Report aufgeführt werden sollen.

   Standardmäßig zeigt der Report alle Benutzer und die zugehörigen Ereignisse an. Sie können den Report aber auch so konfigurieren, dass nur Folgendes angezeigt wird:

   - die obersten *n* Benutzer, für die die meisten Ereignisse verzeichnet wurden (wobei *n* eine von Ihnen festgelegte Anzahl ist) oder
   - Benutzer mit mindestens *m* Ereignissen (wobei *m* eine von Ihnen festgelegte Anzahl ist).

5. Wählen Sie unter **Sortieren nach** aus, ob Sie die Benutzer nach der Ereignisanzahl oder nach Namen sortieren möchten.

   Als Standard listet der Report die Benutzer absteigend nach der Anzahl der zugehörigen Ereignisse auf. Markieren Sie **Benutzer**, wenn die Benutzer alphabetisch aufgelistet werden sollen.

6. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

10.10 Konfigurieren des Reports „Schutz verwalteter Endpoints“

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Im Report **Schutz verwalteter Endpoints** wird der prozentuale Anteil oder die Anzahl der geschützten Computern in regelmäßigen Abständen zusammengefasst.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** die Option **Schutz verwalteter Endpoints** aus und klicken Sie auf **Eigenschaften**.
3. Wählen Sie im Dialogfeld **Schutz verwalteter Endpoints – Eigenschaften** auf der Registerkarte **Konfiguration** die gewünschten Optionen aus.

   a) Im Fenster **Report-Kennung** können Sie auf Wunsch den Namen und die Beschreibung des Reports bearbeiten.

   b) Klicken Sie im Fenster **Reporting-Zeitraum** im Textfeld **Zeitraum** auf den Pfeil des Dropdown-Menüs und wählen Sie den gewünschten Zeitraum aus.

      Sie können entweder einen festen Zeitraum (z.B. **Letzter Monat**) angeben oder die Option **Benutzerdefiniert** wählen und den gewünschten Zeitraum in die Textfelder **Start** und **Ende** eingeben.

   c) Wählen Sie im Fenster **Anzeigen** die Funktionen aus, die im Report aufgeführt werden sollen.

4. Geben Sie auf der Registerkarte **Anzeigeoptionen** unter **Häufigkeit der Ergebnisanzeige** an, wie oft Nichtkonformität festgestellt werden soll (z.B. jede Stunde oder jeden Tag). Klicken Sie auf den Dropdown-Pfeil und wählen Sie ein Intervall aus.
5. Wählen Sie im Bereich **Ergebnisse anzeigen als**, ob die Ergebnisse prozentual oder in Zahlen angezeigt werden sollen.

6. Wählen Sie auf der Registerkarte **Zeitplan** die Option **Zeitplan für diesen Report erstellen** aus, wenn der Report regelmäßig durchgeführt werden soll. Die Report-Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet. Geben Sie den Start-Zeitpunkt des Reports an (Datum und die Uhrzeit). Geben Sie außerdem die gewünschte Report-Häufigkeit, das Datei-Format und die Sprache sowie die E-Mail-Adressen der gewünschten Empfänger an.

10.11 Update-Hierarchie-Reports

Im **Update-Hierarchie**-Report werden die Update Manager im Netzwerk, die entsprechenden Update-Freigaben sowie die Anzahl der Computer, die von diesen Freigaben Updates beziehen, angezeigt.

Der **Update-Hierarchie**-Report ist nicht konfigurierbar. Sie können den Report anhand der Anweisungen im Abschnitt *Ausführen von Reports* (Seite 232) durchführen.

10.12 Report-Zeitpläne

Bei rollenbasierter Verwaltung müssen Sie hierzu über die Berechtigung **Report-Konfiguration** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Sie können einstellen, dass Reports in regelmäßigen Abständen ausgeführt werden. Die Ergebnisse werden als E-Mail-Anhang an die gewählten Empfänger gesendet.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** den Report aus, für den ein Zeitplan erstellt werden soll und klicken Sie auf **Zeitplan**.
3. Rufen Sie in dem Dialogfeld, das angezeigt wird, die Registerkarte **Zeitplan** auf und wählen Sie die Option **Zeitplan für diesen Report erstellen** aus.
4. Geben Sie einen Startzeitpunkt für die Reporterstellung (Datum und Uhrzeit) sowie die Häufigkeit der Report-Erstellung an.
5. Geben Sie das Format und die Sprache für die Reporterstellung an.
6. Geben Sie die E-Mail-Adressen der Report-Empfänger an.

10.13 Ausführen von Reports

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** den gewünschten Report aus und klicken Sie auf **Ausführen**.

   Das **Reports-Fenster** wird angezeigt.

Sie können das Layout des Reports ändern, den Report ausdrucken oder in eine Datei exportieren.

10.14 Report-Tabellen und -Diagramme

Sie können bestimmte Reports als Tabelle und Diagramme darstellen. Wenn dies der Fall ist, sind im **Report-Fenster**, in dem der Report angezeigt wird, zwei Registerkarten vorhanden: **Tabelle** und **Diagramm**.

1. Klicken Sie in der Symbolleiste auf das Symbol **Reports**.
2. Wählen Sie im Dialogfeld **Report Manager** den gewünschten Report aus, z.B. **Alerts und Ereignisse nach Ort** und klicken Sie anschließend auf **Ausführen**.

   Das **Reports-Fenster** wird angezeigt.

3. Wenn der Report als Tabelle oder Diagramm dargestellt werden soll, wählen Sie die entsprechende Registerkarte aus.

10.15 Drucken von Reports

Klicken Sie zum Drucken eines Reports auf das **Drucker**-Symbol in der Symbolleiste im oberen Bereich des Reports.

10.16 Exportieren eines Reports in eine Datei

So exportieren Sie einen Report in eine Datei:

1. Klicken Sie in der Symbolleiste im oberen Bereich des Reports auf das **Export**-Symbol.

2. Wählen Sie im Dialogfeld **Export-Report** das Dokumenten- oder Tabellenformat, in das Sie den Report exportieren möchten.

   Folgende Optionen stehen zur Verfügung:

   - PDF (Acrobat)
   - HTML
   - Microsoft Excel
   - Microsoft Word
   - Rich Text Format (RTF)
   - Comma Separated Values (CSV)
   - XML

3. Klicken Sie auf die Schaltfläche neben dem Feld **Dateiname**, um einen Speicherort auszuwählen. Geben Sie dann einen Namen ein. Klicken Sie auf **OK**.

10.17 Ändern des Report-Layouts

Sie können das Seitenlayout von Reports ändern. Sie können sich beispielsweise einen Report im Querformat anzeigen lassen.

1. Klicken Sie auf das Seitenlayout-Symbol in der Symbolleiste im oberen Seitenbereich.

2. Geben Sie im Dialogfeld **Seite einrichten** die Seitengröße, die Ränder und die Ausrichtung an. Klicken Sie auf **OK**.

   Der Report wird im gewählten Format angezeigt.

Das Format wird auch beim Drucken oder Exportieren von Reports übernommen.

11 Wiederherstellen des Zugangs zu verschlüsselten Computern

11.1 Wiederherstellen des Zugriffs mit Challenge/Response

Challenge/Response hilft Benutzern, die sich nicht an ihrem Computer anmelden oder nicht auf verschlüsselte Daten zugreifen können. Während eines Challenge/Response-Verfahrens übermittelt der Benutzer einen auf dem Endpoint-Computer erzeugten Challenge-Code an den Helpdesk-Beauftragten. Der Helpdesk-Beauftragte erzeugt einen Response-Code, der den Benutzer zum Ausführen einer bestimmten Aktion auf dem Computer berechtigt.

Für Recovery des Zugriffs mit Challenge/Response müssen folgende Voraussetzungen erfüllt sein:

- Challenge/Response muss in einer Richtlinie zur Festplattenverschlüsselung für die Endpoints aktiviert werden.
- Bei rollenbasierter Verwaltung müssen Sie über die Berechtigung **Korrektur – Verschlüsselungs-Recovery** verfügen. Nähere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).
- Wenn Benutzer ihr Kennwort vergessen haben, muss es vor der Erzeugung des Response-Codes in Active Directory zurückgesetzt werden.
- Wenn die POA beschädigt ist und sich der Benutzer nicht anmelden kann, stellen Sie sicher, dass die Schlüssel-Recovery-Datei exportiert wurde und in der Benutzerumgebung verfügbar ist, um das Challenge/Response-Verfahren einleiten zu können (nähere Anweisungen entnehmen Sie bitte dem Abschnitt *Exportieren der Schlüssel-Recovery-Datei* (Seite 236)).

1. Der Benutzer leitet ein Challenge/Response-Verfahren auf dem Endpoint ein, erzeugt einen Challenge-Code und setzt sich mit Ihnen in Verbindung.

   Nähere Informationen zum Einleiten eines Challenge/Response-Verfahrens bei vergessenen Kennwörtern entnehmen Sie bitte der *Sophos Disk Encryption Benutzerhilfe*. Nähere Informationen zum Einleiten eines Challenge/Response-Verfahrens bei beschädigter POA entnehmen Sie bitte der *Sophos Disk Encryption Tools-Anleitung*.

2. Rechtsklicken Sie in der **Computerliste** auf den gewünschten Computer und wählen Sie **Verschlüsselungs-Recovery**.

   Der **Verschlüsselungs-Recovery-Assistent** wird gestartet.

3. Wählen Sie auf der Seite **Wählen Sie eine Recovery-Methode aus** die erforderliche Recovery-Methode aus und klicken Sie auf **Weiter**.

   - Wenn der Benutzer sein Kennwort vergessen hat, wählen Sie **Kennwort vergessen (Recovery für die Anmeldung)**.
   - Wenn sich der Benutzer aufgrund einer beschädigten POA nicht anmelden kann, wählen Sie **Power-on Authentication beschädigt (Schlüssel-Recovery)**.

4. Geben Sie auf der Seite **Geben Sie die Challenge ein** den vom Benutzer bereitgestellten Challenge-Code ein und klicken Sie auf **Weiter**.

   Der Response-Code wird auf der Seite **Teilen Sie dem Endbenutzer die Antwort mit** angezeigt.

5. Teilen Sie dem Endbenutzer den Response-Code mit.

   Wenn Sie den Response-Code telefonisch mitteilen, bietet sich das **Buchstabieralphabet** an.

6. Der Benutzer muss den Response-Code auf dem Endpoint eingeben.

Der Zugriff auf den Endpoint wird wiederhergestellt.

11.1.1 Exportieren der Schlüssel-Recovery-Datei

Bei rollenbasierter Verwaltung müssen Sie über die Berechtigung **Globale Verschlüsselungseinstellungen** verfügen.

Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Mit der Schlüssel-Recovery-Datei wird das Challenge/Response-Verfahren auf dem Endpoint eingeleitet, wenn die POA beschädigt ist und sich der Benutzer nicht am Computer anmelden kann. Die Schlüssel-Recovery-Datei muss exportiert werden. Anweisungen zur Einleitung des Challenge/Response-Verfahrens bei beschädigter POA entnehmen Sie bitte der *Sophos Disk Encryption Tools-Anleitung*.

So exportieren Sie die Recovery-Schlüssel-Datei:

1. Klicken Sie im Menü **Extras** auf **Verschlüsselung verwalten** und wählen Sie **Schlüssel-Recovery-Datei...**.
2. Wählen Sie einen Speicherort für die Schlüssel-Recovery-Datei (*.TOK) aus.
3. Stellen Sie die Recovery-Schlüssel-Datei dem Helpdesk bereit.

11.2 Recovery für den Zugang mit Local Self Help

Mit Local Self Help können sich Benutzer, die ihr Kennwort vergessen haben, ohne Unterstützung des Helpdesks an ihrem Computer anmelden. Benutzer beantworten bei der Anmeldung am Endpoint vordefinierte Fragen in der Power-on Authentication.

Local Self Help muss in einer Richtlinie zur Festplattenverschlüsselung aktiviert werden, damit die Benutzer den Zugang mit Local Self Help wiederherstellen können.

So können Sie den Zugang mit Local Self Help wiederherstellen:

1. Der Benutzer gibt seinen Benutzernamen in der Power-on Authentication auf dem Endpoint ein und klickt auf die Schaltfläche **Recovery**.
2. In den folgenden fünf Dialogen beantwortet der Benutzer eine vordefinierte Anzahl an Fragen, die per Zufallsprinzip aus den auf dem Endpoint gespeicherten Fragen ausgewählt werden. Nach Beantwortung der letzten Frage bestätigt der Benutzer mit **OK**.

3. Im nächsten Dialog kann sich der Benutzer sein Kennwort anzeigen lassen, indem er die Eingabe- oder Leertaste drückt, oder auf die blaue Anzeigebox klickt.

   Das Kennwort wird maximal 5 Sekunden lang angezeigt. Danach wird der Bootvorgang automatisch fortgesetzt. Der Benutzer kann sein Kennwort sofort verbergen, indem er die Eingabe- oder Leertaste drückt, oder auf die blaue Anzeigebox klickt.

4. Wenn der Benutzer das Kennwort gelesen hat, klickt er auf **OK**.

Der Benutzer wird an der Power-on Authentication und an Windows angemeldet und kann das Kennwort für zukünftige Anmeldevorgänge verwenden.

12 Kopieren und Drucken von Daten mit Enterprise Console

12.1 Kopieren von Daten aus der Computerliste

Sie können Daten aus der Computerliste der Ansicht **Endpoints** über die Zwischenablage in ein anderes Dokument kopieren. Die Daten werden durch Tabulatoren voneinander getrennt.

1. Wählen Sie in der Ansicht **Endpoints** im Bereich **Gruppen** die Computergruppe, deren Details kopiert werden sollen.
2. Wählen Sie im Dropdown-Menü **Ansicht** die gewünschten Computer aus, z.B. **Computer mit potenziellen Problemen**.
3. Wenn die Gruppe auch Untergruppen enthält, wählen Sie, ob Computer **Nur auf dieser Ebene** oder **Diese Ebene und abwärts** angezeigt werden sollen.
4. Wählen Sie in der Computerliste die gewünschte Kategorie, z.B. **Antivirus-Details**.
5. Klicken Sie in die Liste, um sie in den Vordergrund zu bringen.
6. Klicken Sie im Menü **Ändern** auf **Kopieren**. Die Daten werden nun in die Zwischenablage kopiert.

12.2 Drucken von Daten aus der Computerliste

Die Informationen der Computerliste in der Ansicht **Endpoints** lassen sich auch ausdrucken.

1. Wählen Sie in der Ansicht **Endpoints** im Bereich **Gruppen** die Computergruppe, deren Details gedruckt sollen.
2. Wählen Sie im Dropdown-Menü **Ansicht** die gewünschten Computer aus, z.B. **Computer mit potenziellen Problemen**.
3. Wenn die Gruppe auch Untergruppen enthält, wählen Sie, ob Computer **Nur auf dieser Ebene** oder **Diese Ebene und abwärts** angezeigt werden sollen.
4. Wählen Sie in der Computerliste die gewünschte Kategorie, z.B. **Antivirus-Details**.
5. Klicken Sie in die Liste, um sie in den Vordergrund zu bringen.
6. Klicken Sie im Menü **Datei** auf **Drucken**.

12.3 Kopieren der Computer-Details eines Computers

Sie können die Daten aus dem Dialogfeld **Computer-Details** in die Zwischenablage kopieren und in ein anderes Dokument einfügen. Aus den Computer-Details gehen der Computername, das Betriebssystem des Computers, die Versionen der installierten Sicherheitssoftware, ausstehende Alerts und Fehler, der Update-Statusversionen usw. hervor.

1. Doppelklicken Sie in der Ansicht **Endpoints** in der Computerliste auf den Computer, dessen Daten kopiert werden sollen.
2. Klicken Sie im Dialogfeld **Computer-Details** auf **Kopieren**, um die Daten in die Zwischenablage zu kopieren.

12.4 Drucken der Computer-Details eines Computers

Sie können die Informationen des Dialogfelds **Computer-Details**. Aus den Computer-Details gehen der Computername, das Betriebssystem des Computers, die Versionen der installierten Sicherheitssoftware, ausstehende Alerts und Fehler, der Update-Statusversionen usw. hervor.

1. Doppelklicken Sie in der Ansicht **Endpoints** in der Computerliste auf den Computer, dessen Daten ausgedruckt werden sollen.
2. Klicken Sie im Dialogfeld **Computer-Details** auf **Drucken**.

13 Fehlersuche

13.1 Keine Durchführung von On-Access-Scans

Verfahren Sie wie folgt, wenn On-Access-Scans nicht auf Computern durchgeführt werden:

1. Stellen Sie fest, welche Anti-Virus- und HIPS-Richtlinie von den Computern genutzt wird.
   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Stellen Sie sicher, dass On-Access-Scans in der Richtlinie aktiviert sind und die Computer richtlinienkonform sind.
   Nähere Informationen hierzu finden Sie unter *Aktivieren/Deaktivieren der On-Access-Scans* (Seite 101) und *Durchsetzen von Gruppenrichtlinien* (Seite 38).

13.2 Die Firewall ist deaktiviert

Wenn die Firewall auf einigen Computern deaktiviert ist:

1. Prüfen Sie, welche Firewall-Richtlinie von den Computern verwendet wird.
   Mehr dazu erfahren Sie unter *Welche Richtlinien sind einer Gruppe zugewiesen?* (Seite 31).
2. Stellen Sie sicher, dass die Firewall in der Richtlinie aktiviert wird und die Computer richtlinienkonform sind.
   Nähere Informationen hierzu finden Sie unter *Vorübergehende Deaktivierung der Firewall* (Seite 123) und *Durchsetzen von Gruppenrichtlinien* (Seite 38).

13.3 Firewall nicht installiert

Hinweis: Bei rollenbasierter Verwaltung ist zur Installation der Firewall die Berechtigung **Computersuche, -schutz und -gruppen** erforderlich. Weitere Informationen finden Sie unter *Rollen und Teilverwaltungseinheiten* (Seite 17).

Überprüfen Sie vor der Installation der Client Firewall auf Endpoints zunächst, ob die Computer unter Windows-Client-Betriebssystemen laufen (Windows 2000 oder höher).

Hinweis: Sie können die Firewall nicht auf Computern mit Server-Betriebssystemen oder Windows Vista Starter installieren.

Verfahren Sie wie folgt, wenn Sie die Firewall auf Computern installieren möchten:

1. Wählen Sie die gewünschten Computer aus, rechtsklicken Sie auf die Auswahl und wählen Sie **Computer schützen**.
   Der **Assistent zum Schutz von Computern** wird gestartet. Klicken Sie auf **Weiter**.
2. Wählen Sie bei entsprechender Aufforderung die Option **Firewall**. Beenden Sie den Assistenten.

Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support von Sophos.

13.4 Computer mit ausstehenden Alerts

- Befindet sich auf Computern ein Virus oder eine unerwünschte Anwendung, verfahren Sie anhand der Anweisungen im Abschnitt *Sofortiges Bereinigen von Computern* (Seite 64).
- Wenn Computer jedoch Adware oder eine potenziell unerwünschte Anwendung umfassen, die *erwünscht* ist, befolgen Sie die Anweisungen im Abschnitt *Zulassen von Adware und PUA* (Seite 97).
- Bei nicht aktuellen Computern finden Sie im Abschnitt *Updaten nicht aktueller Computer* (Seite 92) Anweisungen zur Fehlersuche und Problembehebung.

Hinweis: Wenn der Alert nicht mehr angezeigt werden soll, können Sie ihn löschen. Markieren Sie die Computer mit Alerts, rechtsklicken Sie auf die Auswahl und wählen Sie **Alerts und Fehler löschen**. Sie müssen zur **Korrektur – Bereinigung** berechtigt sein, um Fehler und Alerts löschen zu können.

13.5 Computer werden nicht von der Konsole verwaltet

Windows-, Mac-, Linux- und UNIX-Computer sollten von Enterprise Console verwaltet werden, so dass sie aktualisiert und überwacht werden können.

Hinweis: Wenn Sie keine Synchronisierung über Active Directory durchgeführt haben (siehe *Informationen zur Synchronisierung mit Active Directory* (Seite 41)), werden neue Netzwerkcomputer nicht automatisch von der Konsole angezeigt bzw. verwaltet. Klicken Sie in der Symbolleiste auf **Computer ermitteln**, um nach diesen Computern zu suchen und sie in der Gruppe **Nicht zugewiesen** abzulegen.

Wenn ein Computer nicht verwaltet wird, werden seine Details auf der Registerkarte **Status** grau angezeigt.

So können nicht verwaltete Computer verwaltet werden:

1. Wählen Sie im Dropdown-Menü **Ansicht** die Option **Nicht verwaltete Computer**.
2. Markieren Sie alle aufgelisteten Computer. Rechtsklicken Sie auf die Auswahl und wählen Sie **Computer schützen**, um eine verwaltete Version von Sophos Endpoint Security and Control zu installieren.
3. Führen Sie auf Computern, auf denen Enterprise Console Endpoint Security and Control nicht automatisch installieren kann, eine manuelle Installation durch.

   Nähere Anweisungen entnehmen Sie bitte der Erweiterten *Startup-Anleitung* zu Sophos Enterprise Console.

13.6 Schutz von Computern in der Gruppe „Nicht zugewiesen“ nicht möglich

Die Gruppe **Nicht zugewiesen** ist für Computer gedacht, die noch in keine Gruppe eingegliedert wurden und auf die sich Richtlinien übertragen lassen. Computer werden erst geschützt, wenn sie sich in einer Gruppe befinden.

13.7 Sophos Endpoint Security and Control konnte nicht installiert werden

Wenn der **Assistent zum Schutz von Computern** Sophos Endpoint Security and Control nicht auf Computern installieren kann, kann dies folgende Ursache haben:

- Enterprise Console konnte das Betriebssystem der Computer nicht ermitteln. Sie haben wahrscheinlich beim Suchen von Computern Ihren Benutzernamen nicht im Format „Domäne\Benutzer“ eingegeben.
- Auf dem Betriebssystem ist eine automatische Installation nicht möglich. Führen Sie eine manuelle Installation durch. Nähere Anweisungen entnehmen Sie bitte der Erweiterten *Startup-Anleitung* zu Sophos Enterprise Console.
- Die Computer werden von einer Firewall geschützt.
- Die „Einfache Dateifreigabe“ wurde auf Windows XP-Computern nicht deaktiviert.
- Die Option „Freigabe-Assistent verwenden“ wurde unter Windows Vista nicht deaktiviert.
- Sie haben eine Funktion ausgewählt, die nicht auf diesem Betriebssystem unterstützt wird.

Wenn die Installation von Compliance Control nicht durchgeführt werden kann oder ein Fehler auftritt, können Sie das Compliance Control-Installationsprotokoll aufrufen. Das Protokoll befindet sich im Ordner %tmp%.

Die Systemvoraussetzungen für Sophos Endpoint Security and Control entnehmen Sie bitte der Sophos Website: *http://www.sophos.de/products/all-sysreqs.html*.

13.8 Computer werden nicht upgedatet

Im Abschnitt *Updaten nicht aktueller Computer* (Seite 92) finden Sie Hinweise zur Fehlersuche und Problembehebung.

13.9 Virenschutzeinstellungen werden von Macintosh-Computern nicht übernommen

Manche Virenschutzeinstellungen können von Macintosh-Computern nicht übernommen werden. In diesem Fall wird auf der entsprechenden Seite eine Warnung angezeigt.

Sie können Virenschutzeinstellungen auf Mac-Computern mithilfe des Sophos Update Managers ändern, einem Dienstprogramm, das mit Sophos Anti-Virus für Mac OS X geliefert wird. Um den Sophos Update Manager auf einem Mac-Computer zu öffnen, suchen Sie in einem **Finder**-Fenster nach dem Ordner „Sophos Anti-Virus:ESOSX“. Doppelklicken Sie auf **Sophos Update Manager**. Weitere Details werden in der Hilfe zu Sophos Update Manager aufgeführt.

13.10 Virenschutzeinstellungen werden von Linux oder UNIX nicht übernommen

Manche Virenschutzeinstellungen können von Linux- oder UNIX-Computern nicht übernommen werden. In diesem Fall wird auf der entsprechenden Seite eine Warnung angezeigt.

Sie können die Virenschutzeinstellungen unter Linux über die Befehle **savconfig** und **savscan** ändern. Nähere Anweisungen hierzu finden Sie im Benutzerhandbuch zu Sophos Anti-Virus für Linux. Sie können Virenschutzeinstellungen unter UNIX über den Befehl **savscan** ändern. Nähere Anweisungen hierzu finden Sie im *Benutzerhandbuch* für Sophos Anti-Virus für UNIX.

13.11 Linux- oder UNIX-Computer stimmt nicht mit Richtlinie überein

Wenn Sie eine Unternehmens-Konfigurationsdatei im zentralen Installationsverzeichnis verwenden und die Datei einen Konfigurationseintrag enthält, der mit der Richtlinie in Konflikt steht, wird der Computer als nicht richtlinienkonform angezeigt.

Wenn Sie die Option **Konformität mit Richtlinie** wählen, wird der Computer nur vorübergehend in Übereinstimmung gebracht, bis die CID-basierte Konfiguration erneut übertragen wird.

Prüfen Sie die Unternehmens-Konfigurationsdatei und ersetzen Sie die Konsolen-basierte Konfiguration, falls möglich.

13.12 Unerwarteter Scan unter Windows 2000 oder höher

Bei einer lokalen Version von Sophos Anti-Virus unter Windows 2000 oder höher wird eventuell ein „verfügbarer Scan“ in der Liste aufgeführt, obwohl der Benutzer keinen erstellt hat.

Bei dem neuen Scan handelt es sich eigentlich um einen geplanten Scan, den Sie von der Konsole aus eingerichtet haben. Löschen Sie den Scan nicht.

13.13 Verbindungs- und Zeitüberschreitungsprobleme

Wenn die Kommunikation zwischen Enterprise Console und einem Computer im Netzwerk langsam wird oder der Computer nicht reagiert, kann ein Verbindungsproblem bestehen.

Sehen Sie im Sophos Netzwerkkommunikations-Report nach, der einen Überblick über den aktuellen Kommunikationsstatus zwischen einem Computer und Enterprise Console bietet. Um den Report anzusehen, gehen Sie zu dem Computer, auf dem das Problem aufgetreten ist. Klicken Sie in der Taskleiste auf die Schaltfläche **Start** und wählen Sie dann **Programme** > **Sophos** > **Sophos Endpoint Security and Control** und klicken Sie auf **Sophos Netzwerkkommunikations-Report ansehen**.

Der Report zeigt mögliche Problemursachen an. Wenn ein Problem erkannt wird, werden Abhilfemaßnahmen vorgeschlagen.

13.14 Adware/PUA werden nicht erkannt

Wenn Adware und andere potenziell unerwünschte Anwendungen (PUA) nicht erkannt werden, prüfen Sie Folgendes:

- Die Erkennung wurde aktiviert. Mehr dazu erfahren Sie unter *Scannen auf Adware und PUA* (Seite 96).
- Anwendungen werden auf einem Computer unter Windows 2000 oder höher ausgeführt.

13.15 Zum Teil erkanntes Objekt

Sophos Endpoint Security and Control kann melden, dass ein Objekt (z.B. ein Trojaner oder eine potenziell unerwünschte Anwendung) zum Teil erkannt wurde. Das bedeutet, dass Sophos Anti-Virus nicht alle Komponenten dieser Anwendung gefunden hat.

Die verbleibenden Komponenten können Sie über eine vollständige Systemüberprüfung der betroffenen Computer auffinden. Auf Computern unter Windows 2000 und höher können Sie hierzu den/die Computer auswählen, darauf rechtsklicken und **Vollständige Systemüberprüfung** wählen. Sie können außerdem einen geplanten Scan zur Erkennung von Adware und anderen potenziell unerwünschten Anwendungen einrichten. Mehr dazu erfahren Sie unter *Scannen auf Adware und PUA* (Seite 96).

Wenn die Anwendung noch immer nicht vollständig erkannt wurde, kann es dafür folgende Gründe geben:

- Sie haben keine ausreichenden Zugriffsrechte.
- Einige Laufwerke oder Ordner auf dem Computer, die die Komponenten der Anwendung enthalten, sind vom Scan ausgeschlossen.

In letzterem Fall prüfen Sie die Liste der vom Scan ausgeschlossenen Objekte (mehr dazu erfahren Sie unter *Ausschließen von Objekten von On-Access-Scans* (Seite 103)). Wenn die Liste Objekte enthält, entfernen Sie diese und wiederholen Sie den Scan-Vorgang.

Sophos Endpoint Security and Control kann Adware und potenziell unerwünschte Anwendungen, deren Komponenten auf Netzlaufwerken installiert wurden, eventuell nicht vollständig erkennen oder entfernen.

Wenn Sie Hilfe benötigen, wenden Sie sich bitte an den technischen Support von Sophos.

13.16 Hohe Alert-Anzahl aufgrund potenziell unerwünschter Anwendungen

Es kann vorkommen, dass zahlreiche Alerts aufgrund potenziell unerwünschter Anwendungen ausgegeben werden, die sich unter Umständen jedoch auf die gleiche Anwendung beziehen.

Ursache dafür kann sein, dass einige Arten potenziell unerwünschter Anwendungen Dateien "überwachen" und versuchen, häufig auf sie zuzugreifen. Bei aktiviertem On-Access-Scanning erkennt Sophos Endpoint Security and Control jeden Dateizugriff und gibt einen Alert aus.

Führen Sie einen der folgenden Schritte durch:

- Deaktivieren Sie On-Access-Scans auf Adware/PUA. Sie können stattdessen einen geplanten Scan verwenden.
- Lassen Sie die Anwendung zu (wenn sie auf Ihren Computern ausgeführt werden soll). Mehr dazu erfahren Sie unter *Zulassen von Adware und PUA* (Seite 97).
- Bereinigen Sie die Computer, indem Sie Anwendungen entfernen, die Sie nicht zugelassen haben. Mehr dazu erfahren Sie unter *Sofortiges Bereinigen von Computern* (Seite 64).

13.17 Bereinigung fehlgeschlagen

Wenn Endpoint Security and Control Objekte nicht bereinigen kann („Bereinigung fehlgeschlagen"), kann es dafür folgenden Grund geben:

- Das Programm hat nicht alle Komponenten eines aus mehreren Komponenten bestehenden Objekts gefunden. Führen Sie eine vollständige Systemüberprüfung der Computer durch, um die anderen Komponenten zu suchen. Mehr dazu erfahren Sie unter *Sofort-Scans* (Seite 63).
- Einige Laufwerke oder Ordner, die Komponenten des Objekts enthalten, wurden vom Scan-Vorgang ausgeschlossen. Prüfen Sie die von der Scan-Vorgang ausgeschlossenen Objekte. Anweisungen hierzu Sie unter *Ausschließen von Objekten von On-Access-Scans* (Seite 103). Wenn sich Objekte in der Liste befinden, entfernen Sie diese.
- Sie haben keine ausreichenden Zugriffsrechte.
- Die Software kann diese Objektart nicht bereinigen.
- Sophos Anti-Virus hat ein Virenfragment anstelle einer genauen Virenübereinstimmung entdeckt.
- Das Objekt befindet sich auf einer schreibgeschützten Diskette oder CD.
- Das Objekt befindet sich auf einem schreibgeschützten NTFS-Volume (Windows 2000 oder höher).

13.18 Wiederherstellung bei Folgeerscheinungen von Viren

Eine Bereinigung kann zwar einen Virus vom Computer entfernen, aber nicht immer die Folgeerscheinungen rückgängig machen.

Bei einigen Viren treten keine Folgeerscheinungen auf. Andere können Änderungen vornehmen oder Daten so beschädigen, dass sie schwer zu erkennen sind. Gehen Sie damit folgendermaßen um:

- Klicken Sie im **Hilfe**-Menü auf **Sicherheitsinformationen**. Dadurch werden Sie mit der Sophos Website verbunden, auf der Sie die Virenanalyse lesen können.
- Ersetzen Sie infizierte Programme durch Sicherungskopien oder Original-Programme. Wenn Sie vor der Infektion keine Sicherungskopien hatten, sollten Sie diese jetzt auf jeden Fall für die Zukunft erstellen.

Manchmal lassen sich jedoch noch Daten auf von Viren beschädigten Festplatten retten. Sophos verfügt über Tools zur Behebung bestimmter Virenschäden. Der technische Support kann Ihnen bei der Problembehebung behilflich sein.

13.19 Wiederherstellung nach Folgeerscheinungen unerwünschter Anwendungen

Eine Bereinigung kann zwar unerwünschte Anwendungen von dem Computer entfernen aber nicht immer die Folgeerscheinungen rückgängig machen.

Durch bestimmte Anwendungen werden Änderungen am Betriebssystem vorgenommen (z.B. werden Einstellungen der Internetverbindung modifiziert). Sophos Endpoint Security and Control kann nicht immer alle Einstellungen wiederherstellen. Wenn beispielsweise eine Anwendung die Browser-Startseite geändert hat, kennt Sophos Endpoint Security and Control die vorherige Einstellung nicht.

Einige Anwendungen installieren Dienstprogramme auf Ihrem Computer, wie z.B. .dll- oder .ocx-Dateien. Wenn ein Dienstprogramm harmlos (d.h. dass es nicht die Eigenschaften einer potenziell unerwünschten Anwendung besitzt), z.B. eine Sprach-Library, und kein wesentlicher Teil der Anwendung ist, erkennt es Sophos Endpoint Security and Control möglicherweise nicht als Teil der Anwendung. In diesem Fall wird die Datei durch eine Bereinigung nicht aus Ihrem Computer entfernt.

Manchmal ist eine Anwendung, wie Adware, Teil eines Programms, das Sie absichtlich installiert haben, und für die Funktion des Programms erforderlich. Wenn Sie die Anwendung entfernen, funktioniert das Programm auf Ihrem Computer möglicherweise nicht mehr.

Gehen Sie folgendermaßen vor:

- Klicken Sie im **Hilfe**-Menü auf **Sicherheitsinformationen**. Dadurch werden Sie mit der Sophos Website verbunden, auf der Sie die Anwendungsanalyse lesen können.
- Stellen Sie die gewünschten Systemeinstellungen oder Programme über Sicherungskopien wieder her. Wenn Sie noch keine Sicherungskopien erstellt haben, sollten Sie diese jetzt auf jeden Fall für die Zukunft erstellen.

Der technische Support von Sophos kann Ihnen Hilfe oder weitere Hinweise zur Wiederherstellung bei Folgeerscheinungen von Adware/potenziell unerwünschten Anwendungen bereitstellen.

13.20 Data Control erkennt keine Dateien, die über integrierte Browser hochgeladen wurden

Data Control fängt Dokumente ab, die über eigenständige Browser hochgeladen werden. Dokumente, die über in Fremdsoftware integrierte Browser (z.B. Lotus Notes) hochgeladen werden, werden jedoch nicht erkannt. Wenn Sie über Software mit einem integrierten Browser arbeiten und hochgeladene Dokumente überprüfen möchten, müssen Sie in Ihrer Software einstellen, dass die Anwendung in einem externen Browser geöffnet wird.

13.21 Data Contorl scannt hochgeladene oder angehängte Dateien nicht

Wenn Data Control Dateien, die mit einer überwachten Anwendung, z.B. einem E-Mail-Client, Browser oder Instant Messaging-Client im Netzwerk hochgeladen oder angehängt wurden, nicht erfasst, haben Sie möglicherweise Remote-Dateien in der Antivirus- und HIPS-Richtlinie von On-Access-Scans ausgeschlossen. Data Control verwendet die gleichen Ausschlüsse wie der On-Access-Scanner von Sophos Anti-Virus: Wenn das Scannen von Remote-Dateien also deaktiviert wurde, werden keine Remote-Dateien an Data Control gesendet.

Weitere Informationen zum Konfigurieren von Ausschlüssen zu On-Access-Scans entnehmen Sie bitte dem Abschnitt *Ausschließen von Objekten von On-Access-Scans* (Seite 103).

Hinweis: Diese Einschränkung gilt nicht für die Überwachung von Speichergeräten. Data Control unterbricht die Übertragung von Dateien auf überwachte Speichergeäte aus dem Netzwerk (z.B. das Kopieren von Dateien auf ein Wechselmedium oder Brennen auf optische Medien).

13.22 Der deinstallierte Update Manager wird in der Konsole angezeigt

Wenn Sie einen weiteren Update Manager deinstalliert haben, wird er bisweilen noch in der Ansicht **Update Manager** in Enterprise Console angezeigt.

Um den Update Manager aus der Konsole zu entfernen, rechtsklicken Sie darauf und wählen Sie **Löschen**.

14 Glossar

Active Directory-Synchronisierungsereignis	Ereignis, das bei einer Active Directory-Synchronisierung auftritt.
Advanced Content Control List Editor	Editor zum Erstellen benutzerdefinierter „Content Control Lists". „Content Control Lists" umfassen die Komponenten: „Bewertung", „Höchstzahl", „regulärer Ausdruck" sowie die sog. „Schwellenbewertung", die erzielt werden muss, damit eine Übereinstimmung mit der Content Control List vorliegt.
Aktive Teilverwaltungseinheit	Eine im Gruppenfenster angezeigte Teilverwaltungseinheit.
Application Manager	In diesem Fenster lassen sich neue Regeln für von Sophos Client Firewall gesperrte Anwendungen erstellen.
Ausdruck	Siehe unter „regular Expression".
Automatischer Schutz	Installation von Sicherheitssoftware und Richtliniendurchsetzung auf allen Computern in einem Active Directory-Container nach Synchronisierung mit Enterprise Console.
Beispielregel	Regel, die Sophos als Beispiel zur Verfügung stellt. Diese Regeln werden nicht von Sophos aktualisiert.
Benutzerdefinierte Content Control List	Von einem Sophos Kunden erstellte Content Control List. Benutzerdefinierte Content Control Lists können wie folgt erstellt werden: Erstellen Sie eine einfache Liste mit Suchbegriffen und einem Suchparameter (z.B. „nach allen Begriffen"). Sie können jedoch auch den „Advanced Content Control List Editor" verwenden.
Bewertung	Zahl, die zur Gesamtbewertung einer Content Control List addiert wird, wenn eine Übereinstimmung zu einem regulären Ausdruck vorliegt.
Challenge/Response (C/R)	Recovery-Methode bei Festplattenverschlüsselung, die den Benutzern die Anmeldung an ihren Computern erleichtert, wenn sie ihr Kennwort vergessen haben oder nicht mehr auf verschlüsselte Daten zugreifen können. Die Unterstützung des Helpdesks ist erforderlich.
Content Control List (CCL)	Eine Kombination von Bedingungen zur Bestimmung des Inhalts von Dateien (z.B.

	Kreditkarten- oder Kontodaten oder andere personenbezogenen Daten). Es wird zwischen zwei Arten von „Content Control Lists“ unterschieden: „SophosLabs Content Control Lists“ und „benutzerdefinierte Content Control Lists“.
Controlled Application	Anwendung, die aus Gründen der Produktivitätsbeeinträchtigung oder Netzwerkbelastung als unerwünscht betrachtet wird und deshalb gesperrt werden soll.
Controlled Data	Dateien, die Data Control-Bedingungen erfüllen.
Controlled Device	Ein von der Funktion „Device Control“ überwachtes Gerät.
Dashboard	Übersichtliche Darstellung der Netzwerksicherheit.
Dashboard-Ereignis	Auf dem Dashboard angezeigtes Ereignis, wenn eine kritische Sicherheitsstufe überschritten wurde. In diesem Fall wird eine E-Mail-Benachrichtigung erzeugt und verschickt.
Data Control	Kontrollfunktion zur Verhinderung, dass ungewollt Daten von Computern übertragen werden. Der Mechanismus greift, wenn ein Benutzer eine Datei versenden oder anderweitig übertragen möchte, die die Kriterien der „Data Control“-Richtlinie und der entsprechenden Regeln erfüllt. Wird beispielsweise eine Tabelle mit Kundendaten auf einen Wechseldatenträger kopiert oder ein vertrauliches Dokument in einem webbasierten E-Mail-Konto hochgeladen, wird die Übertragung bei entsprechender Konfiguration verhindert.
Dateiregel	Regel zum Bestimmen der zu ergreifenden Maßnahme, wenn ein Benutzer eine Datei mit dem festgelegten Namen oder Typ an das festgelegte Ziel übertragen möchte (z.B. Verhindern der Übertragung von Datenbanken an Wechseldatenträger).
Datenbanken	Komponente von Sophos Enterprise Console, in der alle Daten über die Netzwerkcomputer gespeichert werden.
Device Control	Eine Funktion zur Reduzierung ungewünschter Datenverluste über Computer und Einschränkung der Einführung von Software in das Netzwerk von außerhalb. Diese Funktion spricht an bei Zugriff auf ein nicht zugelassenes Speicher- oder

	Netzwerkgerät auf einem verwalteten Computer im Netzwerk.
Echter Dateityp	Dateityp, der durch Strukturanalyse und nicht anhand der Dateierweiterung ermittelt wird. Diese Methode liefert bessere Ergebnisse.
Erkennung verdächtigen Verhaltens	Dynamische Analyse des Verhaltens aller auf einem System ausgeführten Programme. Bei Erkennung von Schadenspotenzial wird das jeweilige Programm an der Ausführung gehindert.
Festplattenverschlüsselung	Funktion zum Schutz von Daten auf Endpoints davor, von nicht autorisierten Personen gelesen oder geändert zu werden.
Geräte-Ausschluss	Ein von der Funktion „Device Control“ nicht zu berücksichtigendes Gerät.
Gesamtbewertung	Alle Bewertungen einer Content Control List, je nach berücksichtigtem Content.
Gruppe	Gruppe von Sophos Enterprise Console verwalteter Computer.
Host Intrusion Prevention System (HIPS)	Sicherheitsverfahren, das Computer vor verdächtigen Dateien, unbekannten Viren und verdächtigem Verhalten schützt.
Höchstzahl	Maximal zugelassene Übereinstimmungen eines regulären Ausdrucks, die in die Gesamtbewertung eingehen.
Inhaltsregel	Eine Inhaltsregel umfasst mindestens eine Content Control List. Hierin wird die Maßnahme festgelegt, die bei der Übertragung von Daten, die alle Bedingungen der Content Control Lists der Regel erfüllen, an den festgelegten Zielort ergriffen werden soll.
IT-Verwaltungseinheit	IT-Umgebung eines Unternehmens, u.a. bestehend aus Computern und Netzwerkinfrastruktur.
Kategorie	Kriterium zur Kategorisierung von Control Lists der SophosLabs Content nach Typ, Content-Regulierung oder Region.
Kriterium	Deskriptor einer SophosLabs Content Control List zum Bestimmen der Inhalte oder des Umfangs der Liste. Es gibt drei Kriterien: Typ, Regulierung und Region.
Kritische Stufe	Dieser Wert ändert den Sicherheitsstatus eines Objekts in „kritisch“.

Local Self Help (LSH)	Recovery-Methode bei Festplattenverschlüsselung, die den Benutzern die Anmeldung an ihren Computern erleichtert, wenn sie ihr Kennwort vergessen haben. Benutzer können sich anmelden, wenn sie im Vorfeld definierte Fragen beantworten. Die Unterstützung des Helpdesks ist nicht erforderlich.
Management-Konsole	Die Komponente von Sophos Enterprise Console zur Verwaltung und zum Schutz von Computern.
Management-Server	Die Komponente von Sophos Enterprise Console zur Abwicklung der Updates und der Kommunikation zwischen Netzwerkcomputern.
Manipulationsschutz	Mit dem Manipulationsschutz können Sie verhindern, dass bekannte Malware sowie nicht autorisierte Benutzer (lokale Administratoren und Benutzer ohne hinreichende Fachkenntnisse) Sophos Sicherheitssoftware deinstallieren bzw. mit Sophos Endpoint Security and Control deaktivieren.
Menge	Anzahl der Content Control List-Schlüsseldaten, die eine Datei umfassen muss, damit eine Übereinstimmung mit der Content Control List vorliegt.
Mengenschlüssel	In der Content Control List festgelegte Schlüsseldaten, deren Menge bestimmt wird. Wenn eine Content Control List beispielsweise Kreditkarten- oder Bankdaten enthält, bestimmen die Mengeneinstellungen, wie viele Daten maximal in der Datei vorhanden sein können, ohne dass eine Übereinstimmung mit der Content Control List vorliegt.
Patch-Analyse	Analyse der auf Computern installierten Patches und Ermitteln fehlender Patches.
Potenziell unerwünschte Anwendung (PUA)	Ein Programm, das an sich nicht schädlich ist, generell aber für die meisten Unternehmensnetzwerke als nicht geeignet angesehen wird.
Power-on Authentication (POA)	Anmeldeverfahren bei Festplattenverschlüsselung, beim der Benutzer sich unmittelbar nach Einschalten des Computers (noch vor dem Starten des Betriebssystems) authentifizieren muss. Erst wenn sich der Benutzer authentifiziert hat, wird das Betriebssystem gestartet und der Benutzer wird an Windows angemeldet.

Recht	Ein Satz von Berechtigungen zum Ausführen bestimmter Aufgaben über Enterprise Console.
Regel	In Regeln werden die Maßnahmen festgelegt, die ergriffen werden, wenn Dateien bestimmte Bedingungen erfüllen. Es wird zwischen Dateiregeln und Inhaltsregeln unterschieden.
Region	Geltungsbereich einer SophosLabs Content Control List. Hier wird das Land festgelegt, auf das sich die Content Control List bezieht (bei länderspezifischen Content Control Lists). Länderunspezifische Content Control Lists werden als „global“ ausgewiesen.
Regulärer Ausdruck	Suchzeichenfolge, die Textmuster in Dateien mit bestimmten Zeichen abgleicht. Data Control arbeitet mit regulärer Ausdruckssyntax von Perl 5.
Richtlinie	Eine Ansammlung von Einstellungen für einen bestimmten Zweck, die auf Computergruppen übertragen werden.
Rolle	Ein Satz von Rechten zur Bestimmung des Zugriffs auf Enterprise Console.
Rollenbasierte Verwaltung	Verteilung von Zugriffsrechten auf bestimmte Computer und Prozesse basierend auf der Rolle eines Benutzers im Unternehmen.
Schwellenbewertung	Erforderliche Trefferanzahl eines regulären Ausdrucks, damit eine Übereinstimmung mit der Content Control List vorliegt.
Schwellenwert	Wert, der den Sicherheitszustand eines Objekts in „Warnung“ oder „kritisch“ ändert.
Server-Stammknoten	Der oberste Knoten einer Gruppenstruktur im Fenster **Gruppen** (einschl. der Gruppe **Nicht zugewiesen**).
Software-Abonnement	Ausgewählte Softwareversionen für unterschiedliche Systeme, die vom Update Manager heruntergeladen und auf dem neuesten Stand gehalten werden. Für jedes System können ausgesuchte Versionen abonniert werden (z.B. „Neueste“ für „Windows 2000 und höher“).
Sophos Live-Schutz	Mit dieser Funktion lässt sich über ein „In-the-Cloud“-Verfahren sofort feststellen, ob eine Datei eine Bedrohung darstellt. Bei Bedarf werden umgehend die in der

	Bereinigungskonfiguration von Sophos Anti-Virus festgelegten Maßnahmen ergriffen.
SophosLabs Content Control List	Von Sophos bereitgestellte und verwaltete Content Control List. Sophos aktualisiert SophosLabs Content Control Lists und erstellt neue Content Control Lists, die in Enterprise Console verfügbar gemacht werden. SophosLabs Content Control Lists können inhaltlich nicht bearbeitet werden. Die Menge dieser Content Control Lists ist jedoch variabel.
Sophos Update Manager (SUM)	Programm zum Download von Sophos Sicherheitssoftware und Updates von Sophos oder einem anderen Update-Server in freigegebene Update-Verzeichnisse.
Standardteilverwaltungseinheit	Teilverwaltungseinheit, deren Stamm der Server-Stammknoten der Gruppenstruktur und der Gruppe **Nicht zugewiesen** ist. Sie wird beim ersten Start von Enterprise Console automatisch angezeigt.
Statusanzeige	Oberbegriff für Symbole, die den Sicherheitszustand eines Dashboards-Objekts oder der Netzwerkintegrität darstellen.
Synchronisierte Gruppe	Eine Gruppe unterhalb des Synchronisierungspunkts.
Synchronisierung mit Active Directory	Einweg-Synchronisierung von Gruppen in Sophos Enterprise Console mit Organisationseinheiten oder Containern von Active Directory.
Synchronisierungsintervall	Zeitraum, nach dessen Ablauf ein Synchronisierungspunkt in Enterprise Console mit dem ausgewählten Active Directory-Container synchronisiert wird.
Synchronisierungspunkt (in Active Directory-Struktur)	Gruppe in Sophos Enterprise Console, in die der Inhalt eines ausgewählten Active Directory-Containers (Gruppen und Computer oder nur Gruppen) zur Synchronisierung verschoben wird, wobei die Struktur unversehrt bleibt.
Systemadministrator	Eine vorkonfigurierte Rolle für die Verwaltung von Sophos Sicherheitssoftware im Netzwerk und Rollen in Enterprise Console. Die Rolle „Systemadministrator“ kann nicht gelöscht, mit neuen Rechten versehen oder

	umbenannt werden. Die Windows-Gruppe „Sophos Full Administrators“ muss Bestandteil der Rolle sein. Andere Benutzer und Gruppen können jedoch hinzugefügt bzw. gelöscht werden.
Teilverwaltungseinheit	Ein benannter Teil der IT-Verwaltungseinheit, der eine Untermenge der Computer und Gruppen ausmacht.
Teilverwaltungseinheitsadministration	Funktion zur Einschränkung der Computer und Gruppen, auf denen Vorgänge ausgeführt werden können.
Transparente Verschlüsselung	Verschlüsselungsverfahren, bei dem Daten ohne Benutzereingriff ver- bzw. entschlüsselt werden. Bei Festplattenverschlüsselung werden Festplatten transparent verschlüsselt.
Typ	Kriterien zur Kategorisierung von SophosLabs Content Control Lists. So wird etwa eine Content Control List, die Ausweisdaten, Postanschrift oder E-Mail-Adressen umfasst, dem Typ „Personally Identifiable Information“ (personenbezogene Daten) zugeordnet.
Update Manager	Siehe unter „Sophos Update Manager“.
Veralteter Computer	Computer mit Sophos Software, die nicht mehr auf dem neuesten Stand ist.
Verdächtige Datei	Datei, die zwar für Viren typische Merkmale aufweist, jedoch nicht schädlich sein muss, da diese Merkmale auch in harmlosen Programmen auftreten können.
Verwalteter Computer	Computer mit Remote Management System (RMS), auf dem über Sophos Enterprise Console Software installiert und aktualisiert werden kann und Berichte erstellt werden können.
Verwaltungseinheit	Siehe unter IT-Verwaltungseinheit.
Wake on LAN (WOL)	Verfahren, bei dem Computer im Netzwerk remote gestartet oder aus dem Schlafmodus aktiviert werden, um geplante Wartungsarbeiten durchzuführen.
Warnstufe	Wert, der die Sicherheitsstufe eines Objekts in „Warnung“ ändert.
Web Control	Funktion zum Festlegen und Durchsetzen von Web-Zugriffs-Richtlinien im Unternehmen sowie zum Aufrufen von Reports zur Web-Aktivität.

	Hiermit kann der Benutzerzugriff auf Websites bestimmter Kategorien gesperrt werden, und es können Warnmeldungen angezeigt werden, wenn der Besuch einer Website einen Verstoß gegen Unternehmensrichtlinien darstellt.
Web-Schutz	Funktion zum Erkennen von Threats auf Websites. Hiermit werden Websites gesperrt, auf denen schädliche Inhalte gehostet wurden. Des Weiteren werden schädliche Downloads verhindert. Der Web-Schutz ist Teil der Antivirus- und HIPS-Richtlinie.

15 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter *http://community.sophos.com/* auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Support-Knowledgebase unter *http://www.sophos.de/support/*.
- Laden Sie Dokumentation zu den Produkten unter *http://www.sophos.de/support/docs/* herunter.
- Senden Sie eine E-Mail an den technischen Support *support@sophos.de* und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Sophos Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

16 Rechtlicher Hinweis

Copyright © 2012 Sophos Limited. Alle Rechte vorbehalten. Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Sophos, Sophos Anti-Virus und SafeGuard sind eingetragene Marken von Sophos Limited, Sophos Group und Utimaco Safeware AG. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.

ACE™, TAO™, CIAO™, and CoSMIC™

ACE[1], TAO[2], CIAO[3], and CoSMIC[4] (henceforth referred to as "DOC software") are copyrighted by Douglas C. Schmidt[5] and his research group[6] at Washington University[7], University of California[8], Irvine, and Vanderbilt University[9], Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source10, free software, you are free to use, modify, copy, and distribute–perpetually and irrevocably–the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us[10] know so we can promote your project in the DOC software success stories[11].

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies[12] around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE[13], TAO[14], CIAO[15], and CoSMIC[16] web sites are maintained by the DOC Group[17] at the Institute for Software Integrated Systems (ISIS)[18] and the Center for Distributed Object Computing of Washington University, St. Louis[19] for the development of open-source software as part of the open-source software community[20]. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly,

and that they waive any claims to copyright or ownership. In addition, submitters acknowledgethat any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, WashingtonUniversity, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me[21] know.

Douglas C. Schmidt[22]

Quellen

1. http://www.cs.wustl.edu/~schmidt/ACE.html
2. http://www.cs.wustl.edu/~schmidt/TAO.html
3. http://www.dre.vanderbilt.edu/CIAO/
4. http://www.dre.vanderbilt.edu/cosmic/
5. http://www.dre.vanderbilt.edu/~schmidt/
6. http://www.cs.wustl.edu/~schmidt/ACE-members.html
7. http://www.wustl.edu/
8. http://www.uci.edu/
9. http://www.vanderbilt.edu/
10. mailto:doc_group@cs.wustl.edu
11. http://www.cs.wustl.edu/~schmidt/ACE-users.html
12. http://www.cs.wustl.edu/~schmidt/commercial-support.html
13. http://www.cs.wustl.edu/~schmidt/ACE.html
14. http://www.cs.wustl.edu/~schmidt/TAO.html
15. http://www.dre.vanderbilt.edu/CIAO/
16. http://www.dre.vanderbilt.edu/cosmic/
17. http://www.dre.vanderbilt.edu/
18. http://www.isis.vanderbilt.edu/
19. http://www.cs.wustl.edu/~schmidt/doc-center.html
20. http://www.opensource.org/
21. mailto:d.schmidt@vanderbilt.edu
22. http://www.dre.vanderbilt.edu/~schmidt/

Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at *http://www.apache.org/licenses/LICENSE-2.0*.

Boost

Version 1.0, 17 August 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Common Public License

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to *support@sophos.com* or via the web at *http://www.sophos.com/support/queries/enterprise.html*. A copy of the license agreement for any such included software can be found at *http://opensource.org/licenses/cpl1.0.php*

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

   The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

WilsonORMapper

Copyright © 2007, Paul Wilson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Index

A

Abonnement-Alerts 201
Abonnements 78
  Auswahl 83
  Hinzufügen 80
Abonnieren von Software 80
Active Directory
  Importieren aus 38
  Synchronisierung 44
  Synchronisierungs-Benachrichtigungen 209
Adware 96
Adware/PUA
  Zulassen 97
Aktivieren des Web-Schutzes 99
Aktivieren von Standort-Roaming 86
Alert-Symbole 59
Alerts 59, 201
  Abonnements 201
  Beheben 60
  E-Mail 203
  Informationen zu erkannten Objekten 62
  Löschen 62
  Netzwerkstatus 209
  Synchronisierung mit Active Directory 209
  Umgang mit 60
  Update Manager 91
alternative Update-Quelle 84
Ändern von Richtlinien 36
Ändern von Rollen 19
Anti-Virus 94
Antivirus- und HIPS-Richtlinie 94
Antivirus-Benachrichtigungen
  Desktop 204
  SNMP 204
Anwendungen
  Hinzufügen 119, 126
  Sperren 129
  Zulassen 119, 125, 127–128
Application Control 153–154
  Benachrichtigung 205
  Ereignisse 212
Application Control-Richtlinie 153
Arbeitsmodus, Wechsel in den interaktiven Modus 124
Archivdateien 113
Assistent zum Schützen von Computern
  Funktionsauswahl 51
  Installation von Verschlüsselungsfunktionen 53
  Zugangsdaten 51, 53
Ausschlüsse 111
  geplante Scans 110
  Importieren/Exportieren 115
  On-Access-Scans 103
Auswahl der Software 71
Auswahl von Abonnements 83
automatische Bereinigung 65–66
automatische Desinfektion 65–66
automatische Updates 82
Automatischer Schutz
  bei Synchronisierung mit Active Directory 46

B

Bandbreite
  Verringern 84, 87
Basis 193
Basisversion von Web Control 194, 197
Beheben von Alerts
  Bereinigungsstatus 60
  Informationen zu erkannten Objekten 62
  zu ergreifende Maßnahmen 60, 62
Benachrichtigung 201
  Application Control 205
  Desktop 204
  SNMP 204
Benutzeroberfläche 4
  Endpoint-Ansicht 9
  Update Manager-Ansicht 13
Benutzeroberfläche von Enterprise Console
  Endpoint-Ansicht 9
  Update Manager-Ansicht 13
Benutzerrollen
  Anzeigen 22
Berechtigungen 22
  Hinzufügen 20
  Zuweisen 20
Bereinigung 60, 64
  automatisch 65–66
  fehlgeschlagen 245
  manuell 65
Bereinigungsstatus 60
Bereitstellung von Software 72
Blockieren 197
Bootstrap-Verzeichnisse 55

C

Challenge/Response 184
Schlüssel-Recovery-Datei 236
Wiederherstellung von Kennwörtern 235
Computer mit aktuellem Schutz
Überprüfen 57
Computer mit Problemen 58
Computer-Details
Drucken 239
Kopieren 238
Computerliste
Drucken von Daten 238
Kopieren von Daten 238
Computersuche
in Enterprise Console 12
Content Control Lists
Ändern mit dem Advanced Editor 169
Bearbeiten 167
Erstellen 167
Erstellen mit dem Advanced Editor 169
Content Control-Inhaltsregeln
Erstellen 163
Controlled Applications
Scannen auf 154
Sperren 154
Controlled Applications, Deinstallieren 155

D

Dashboard
Bereiche 7
Konfigurieren 56
Sicherheitsstatussymbole 8
Data Control
Advanced Content Control List Editor 169
Aktivieren 161
Aktivieren von Data Control 161
Aktivieren/Deaktivieren 161
Ändern von Content Control Lists 167
Ausschließen von Dateien 166
Benachrichtigung 206
CCL 159
Content Control Lists 159
Dateiregeln 161
Entfernen von Regeln aus einer Richtlinie 166
Ereignisse 160, 213
Erstellen von Content Control Lists 167
Exportieren von Content Control Lists 171
Data Control *(Fortsetzung)*
Exportieren von Regeln 167
Hinzufügen von Regeln zu einer Richtlinie 165
Importieren von Content Control Lists 171
Importieren von Regeln 167
Inhaltsregeln 163
Maßnahmen 156
Regelbedingungen 156
Regeln 159
Überblick 156
Data Control-Regeln
Hinzufügen zu einer Richtlinie 165
Datei- und Druckerfreigabe 121
Zulassen 120
Datei- und Druckerfreigabe, Sperren 121
Datei, freigeben 121
Dateifreigabe, sperren 121
Dateiregeln für Data Control
Erstellen 161
Datenverkehr im LAN, Zulassen 120
Deinstallieren von Controlled Applications 155
Desinfektion 64
automatisch 65–66
manuell 65
Desktop-Benachrichtigung 204
Device Control
Ausschließen eines Geräts von allen Richtlinien 176
Ausschließen von Geräten von einer Richtlinie 177
Auswahl der Gerätearten 173
Benachrichtigung 207
Controlled Devices 173
Ereignisse 172, 213
Erkennen und Sperren von Geräten 175
Erkennen und Zulassen von Geräten 174
Liste der ausgeschlossenen Geräte 178
Sperren von Geräten 175
Sperren von Netzwerkbrücken 173
Überblick 171
Download-Scans
Aktivieren 99
Deaktivieren 99
Drucken
Computer-Details 239
Computerlistendaten 238
Drucken von Reports 233
Drucker, freigeben 121
Druckerfreigabe, Sperren 121

E

E-Mail-Benachrichtigungen
Antivirus und HIPS 203
Netzwerkstatus 209
Synchronisierung mit Active Directory 209
Einrichten globaler Regeln 138, 140, 144
Endpoint-Ansicht 9
Drucken von Daten 238
Kopieren von Daten 238
Enterprise Console 4–5, 9
Drucken von Daten 238
Kopieren von Daten 238
Enterprise Console Zugriff 27
Entfernen von Computern aus Gruppen 29
Ereignisprotokoll 210
Ereignisse 212
Application Control 212
Data Control 213
Device Control 213
Exportieren in eine Datei 222
Firewall 214
Manipulationsschutz 216
Patch-Analyse 217
Verschlüsselung 215
Web 220, 222
Erkennen verdächtigen Verhaltens 105
Erkennen von Pufferüberläufen 106
Erkennung schädlichen Verhaltens 105
Ermitteln von Computern 38
im Netzwerk 40
Importieren aus Active Directory 38
Importieren aus einer Datei 41
in einem IP-Bereich 40
mit Active Directory 39
Erstellen von Gruppen 29
Erstellen von Reports 223, 232
Erstellen von Richtlinien 35
Erstellen von Rollen 19
Erstellen von Teilverwaltungseinheiten 20
Erstinstallationsquelle 89
Erweiterungen 111
Exportieren von Reports 233

F

Fehler
Löschen 62
Fehlersuche
ausstehende Alerts 241
Bereinigung 245
Data Control 247
Data Control, integrierte Browser 246
deinstallierter Update Manager 247
Firewall deaktiviert 240
Firewall nicht installiert 240
Gruppe „Nicht zugewiesen“ 241
Linux 243
Mac 242
Nicht aktuelle Computer 242
Nicht verwaltete Computer 241
Objekt zum Teil erkannt 244
On-Access-Scans 240
PUA, Folgeerscheinungen 246
PUA, Hohe Alert-Anzahl 244
PUA, nicht erkannt 244
Sophos Endpoint Security and Control:Installationsproblem 242
UNIX 243
Verbindungsprobleme 243
Virus, Folgeerscheinung 245
Windows 2000 und höher 243
Zeitüberschreitung 243
fehlgeschlagene Bereinigung 245
feste Updates 79
Festlegen der primären Standorte 146
Festplattenverschlüsselung
Challenge/Response 184, 235
Einstellungen 186
Ereignisse 215
Konfigurieren des Anmeldemodus 181
Konfigurieren des Verschlüsselungsmodus 180
Local Self Help 185, 236
Schlüssel-Recovery-Datei 236
Überblick 179
Unternehmenszertifikat 187
Wake on LAN konfigurieren 182
Wake-on LAN konfigurieren 183
Wiederherstellung 235–236
Filtern von ICMP-Meldungen 133
Firewall
Aktivieren 123
Deaktivieren 123
Einrichten 116
Ereignisse 214
Erstellen einer Regel 122, 142
erweiterte Konfiguration 123
Erweiterte Optionen 123

Firewall *(Fortsetzung)*
Hinzufügen von Anwendungen 119, 126
Hinzufügen von Prüfsummen 131
Zulassen der Datei- und Druckerfreigabe 120
Zulassen von Anwendungen 119, 125, 127–128
Firewall-Konfiguration
Exportieren 149
Importieren 149
Freigeben von Sicherheitssoftware in einem Webserver
Internet Information Services (IIS), Verwendung 77

G

geplante Scans 108
Ausschließen von Objekten von 110
Bereinigung 66
Importieren/Exportieren von Ausschlüssen 115
geschützte Computer 56–57
geschütztes Netzwerk 56
Globale Regeln
Einstellung 138, 140, 144
Glossar 248
Gruppe „Nicht zugewiesen“ 28, 241
Gruppen 28
Entfernen von Computern 29
Erstellen 29
Hinzufügen von Computern 29
Importieren aus Active Directory 38
Löschen 30
Nicht zugewiesen 28
Synchronisierung mit Active Directory 44
Umbenennen 30
Verschieben 30
verwendete Richtlinien 31

H

Hinzufügen einer Regel 139–140
Hinzufügen von Anwendungen 119, 126
Hinzufügen von Berechtigungen 20
Hinzufügen von Computern 38
Hinzufügen von Computern zu Gruppen 29
HIPS 94, 104
HIPS-Benachrichtigungen
Desktop 204
E-Mail 203
SNMP 204
Host Intrusion Prevention System 104

I

ICMP-Meldungen
Erläuterung 133
Filtern 133
Importieren von Computern
aus einer Datei 41
In-the-Cloud-Technologie 95
Installationsproblem
Sophos Endpoint Security and Control 242
intelligente Updates 84–85
Aktivieren 86
interaktiver Modus, Aktivieren 124
interaktiver Modus, allgemeine Informationen 124

J

Jetzt scannen 63

K

kategorisierte Updates 79
Konfiguration, Anwenden 147
Konfigurieren
zentrale Reports 147
Richtlinien 33
Konfigurieren des Dashboards 56
Konfigurieren des Update Managers 69
Kopieren
Computer-Details 238
Computerlistendaten 238

L

Laufzeitverhaltensanalyse 104
Local Self Help 185
Wiederherstellung von Kennwörtern 236
Löschen einer Gruppe 30
Löschen von Alerts 62
Löschen von Fehlern 62
Löschen von Richtlinien 37
Löschen von Rollen 19

M

Manipulationsschutz
Aktivieren 188
Ausschalten 188

Manipulationsschutz *(Fortsetzung)*
Deaktivieren 188
Einschalten 188
Ereignisse 187, 216
Kennwortänderung 189
Überblick 187
Manuelle Bereinigung 65
Manuelle Desinfektion 65
manuelle Updates 92

N

NAC 150–152
NAC Manager 151
NAC-Richtlinie 151–152
NAC-Server-URL 151
NAC-URL 151
NAC-Voreinstellungen 151
Network Access Control 150–152
Netzwerkfreigaben
unterstützt 73
Netzwerkstatus-Benachrichtigungen 209
neuer Anwender 27
Nicht aktuelle Computer 242
Auffinden 57
Updates 92
nicht interaktiver Modus, Wechsel in den 125
Nicht verwaltete Computer 241
Nutzungsstatistik 82

O

Objekt zum Teil erkannt 244
On-Access-Scans
Aktivieren 101
Ausschließen von Objekten von 103
Beim Lesen 101
Beim Schreiben 101
Beim Umbenennen 101
Bereinigung 65
Deaktivieren 101
Einschalten 101
Importieren/Exportieren von Ausschlüssen 115

P

Patch-Analyse
Aktivieren 191
Ausschalten 191
Deaktivieren 191
Patch-Analyse *(Fortsetzung)*
Einschalten 191
Ereignisanzeige 216
Ereignisse 191, 217
Intervall 192
Patch-Details 218
Standardeinstellungen 190
Überblick 190
potenziell unerwünschte Anwendungen 96
Power-on Authentication 181
Wiederherstellung 235
Primärserver 84
Ändern der Zugangsdaten 86
Priorität, Scans 115
Prüfsummen 131
PUA 96
Folgeerscheinungen 246
Hohe Alert-Anzahl 244
nicht erkannt 244
Pufferüberläufe
Erkennen 106

R

Raw-Sockets, Zulassen 130
Regel
Hinzufügen 139–140
Regelpriorität 135
Removal Tool
Fremdsoftware 51
Removal-Tool (zur Entfernung von Fremdsoftware) 51
Report-Zeitpläne erstellen 232
Reports
Alert- und Ereignisverlauf 224
Alert-Übersicht 225
Alerts und Ereignisse nach Objektname 226
Alerts und Ereignisse nach Ort 228
Alerts und Ereignisse nach Zeit 227
Ausführen 232
Darstellung als Tabelle 233
Drucken 233
Endpoint-Richtlinienabweichung 229
Endpoint-Schutz nach Zeit 231
Ereignisse nach Benutzer 230
Erstellen 223
Exportieren 233
Layout 234
Richtlinienabweichung nach Uhrzeit 229
Schutz verwalteter Endpoints 231

Reports *(Fortsetzung)*
Überblick 223
Update-Hierarchie 232
Zeitpläne 232
Reports an Sophos 211
Richtlinie 198
Richtlinien 32, 192
Ändern 36
Antivirus und HIPS 94
Durchsetzen 38
Erstellen 35
Festplattenverschlüsselung 179
Konfigurieren 33
Löschen 37
Standard 32
Überblick 31
Überprüfen 37
Übertragen 36
Umbenennen 36
zugehörige Gruppen 37
Zuweisen 36
Rollen 17
Ändern 19
Bearbeiten 19
Erstellen 19
Löschen 19
Umbenennen 19
vordefiniert 18
Zuweisen von Berechtigungen 20
Rootkits
Scannen auf 113

S

Scan-Objekte 111
Scannen auf
verdächtige Dateien 102, 109
Scannen mit niedriger Priorität 115
Scannen von Computern 63
sofort 63
Scans
Ausschlüsse 111
geplant 108
schädliches Verhalten
Erkennen 105
Schaltflächen der Symbolleiste 5
Schutz, Überprüfen 56
Schützen von Computern
Assistent zum Schützen von Computern 51
erforderliche Komponenten, Anti-Virus 49
Schützen von Computern *(Fortsetzung)*
erforderliche Komponenten, Verschlüsselung 49
Funktionsauswahl 51
Vorbereiten der Installation 49
Zugangsdaten 51
sekundäre Konfiguration, Erstellen 146
Sekundärserver 84, 87
Setup 14
SNMP-Benachrichtigungen 204
Sofort-Scan 63
Sofort-Updates 92
Software
Abonnieren von Sicherheitssoftware 80
Auswahl 71
Sophos Endpoint Security and Control
Installationsproblem 242
Sophos Enterprise Console 3, 13
Sophos Live-Schutz
Aktivieren 95
Ausschalten 95
Deaktivieren 95
Einschalten 95
In-the-Cloud-Technologie 95
Überblick 95
Sophos Update Manager 69
Sortieren der Computer-Liste
Computer mit Problemen 58
Ungeschützte Computer 58
Sperren
Anwendungen 129
Controlled Applications 154
Datei- und Druckerfreigabe 121
Spyware 94
Standardeinstellungen globaler Regeln
nähere Informationen 136
Standort-Roaming 84–85
Aktivieren 86
standortspezifische Konfiguration
Einrichten 145
Informationen 145
mit zwei Netzwerkadaptern 145
Starten von NAC Manager 151
Symbole 10
Synchronisierte Gruppe 43
Synchronisierung mit Active Directory 41, 44
Aktivieren 48
Automatischer Schutz 46
Deaktivieren 48
Eigenschaften, ändern 47

Synchronisierungspunkt 43
Systemspeicher scannen 114

T

Teilverwaltungseinheiten 17
aktiv 20
Ändern 20–21
Auswahl 20
Bearbeiten 21
Erstellen 20
Kopieren 21
Löschen 21
Umbenennen 21
Teilverwaltungseinheiten von Benutzern
Anzeigen 22
Trojaner 94

U

Übertragen von Richtlinien 36
Überwachungsmodus 118
Umbenennen von Gruppen 30
Umbenennen von Richtlinien 36
Umgang mit Alerts 60
Ungeschützte Computer 58
Unternehmenszertifikat 187
unterstützte Netzwerkfreigaben 73
Update Manager 69
Alerts
Bereinigen 91
Anzeige der Konfiguration 69
Auswahl einer Update-Quelle 70
Bereitstellung von Software 72
Fehler 90
Hinzufügen 75
Konfigurieren 69
Protokollierung 74
Selbst-Updates 74
Status 90
Übernahme der Konfigurationseinstellungen 75
Übersicht 90
unterstützte Netzwerkfreigaben 73
Updates 75
Zeitpläne 73
zusätzlich 75
Update Manager-Ansicht 13
Update-Arten 79
Update-Quelle 70
alternativ 84
primär 84
sekundär 84, 87
Web-Server 77
Update-Server 69
Update-Zeitplan 73
Updates
Arten 79
automatisch 82
Bandbreite verringern 84, 87
Erstinstallationsquelle 89
feste Updates 79
Freigeben von Sicherheitssoftware in einem Webserver 77
intelligente Updates 84–85
intelligente Updates, Aktivieren 86
kategorisierte Updates 79
manuell 92
Nicht aktuelle Computer 92
Primäre Update-Quelle 84
Primärserver 84
Protokollierung 90
Proxy-Details 84, 87
Sekundäre Update-Quelle 84, 87
Sekundärserver 84, 87
sofort 92
Standort-Roaming 84–85
Standort-Roaming, Aktivieren 86
Zeitpläne 88

V

Verbindungsprobleme 243
verdächtige Dateien
Scannen auf 102, 109
verdächtige Objekte
vorzeitig zulassen 107
Zulassen 107
verdächtiges Verhalten
Erkennen 105
Verhaltensüberwachung 104
Aktivieren 104
Verschlüsselung
Assistent zum Schützen von Computern 53
Challenge/Response 235
Einstellungen 186
Ereignisse 215
Installation 53
Local Self Help 236

Verschlüsselung *(Fortsetzung)*
Power-on Authentication 181
Schlüssel-Recovery-Datei 236
Überblick 179
Wiederherstellung 235–236
Zugangsdaten 53
Versteckte Prozesse, Zulassen 129
verwaltete Computer 10
Viren 94
Viren-Alerts
E-Mail 203
Virus
Folgeerscheinungen 245
Vollständige Systemüberprüfung 63
vom Netzwerk getrennte Computer 10
Vorbereitung 14
vordefinierte Rollen 18
vorzeitig zulassen
verdächtige Objekte 107
Website 99

W

Wake on LAN 182
Wake-on LAN 183
Warnen 197
Warnsymbole 10
Web
Ereignisse 220, 222
Web Appliance 198
Web Control 192–194, 197–198
Web Control-Richtlinie 192
Web-Schutz
Aktivieren 99
Web-Schutz *(Fortsetzung)*
Deaktivieren 99
Überblick 98
Website
vorzeitig zulassen 99
Zulassen 99
Website-Ausschlüsse 197
Website-Kategorien 194, 197
Wiederherstellung 235–236
Schlüssel-Recovery-Datei 236
Würmer 94

Z

Zeitplan für Updates 88
Zeitüberschreitung 243
zentrale Reports, Konfigurieren 147
Zugriff auf Enterprise Console 27
Zulassen 197
Adware/PUA 97
Datei- und Druckerfreigabe 121
Datenverkehr im LAN 120
Raw-Sockets 130
verdächtige Objekte 107
Versteckte Prozesse 129
Website 99
Zulassen der Datei- und Druckerfreigabe 120
Zulassen von Anwendungen 119, 125, 127–128
Zuweisen von Berechtigungen 20
Zuweisen von Richtlinien 36
zwei Netzwerkadapter
Verwenden 145
zwei Standorte 116, 145